

# Network Forensics

## Module 07






## Computer Hacking Forensic Investigator v9

### Module 07: Network Forensics

Exam 312-49



# Module Objectives



→ After successfully completing this module, you will be able to:

- 1 Understand the importance of network forensics
- 2 Discuss the fundamental logging concepts
- 3 Summarize the event correlation concepts
- 4 Understand network forensic readiness and list the network forensics steps
- 5 Examine the Router, Firewall, IDS, DHCP and ODBC logs
- 6 Examine the network traffic
- 7 Document the evidence gathered on a network
- 8 Perform evidence reconstruction for investigation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Network forensics ensures that all the network data flows are instantly visible, enabling monitors to notice insider misuse and advanced threats. This module discusses the importance of network forensics, the analysis of logs from various devices, and investigating network traffic. Network forensics includes seizure and analysis of network events to identify the source of security attacks or other problem incidents by investigating log files.

## Scenario




Jessica was missing from her home for a week. She left a note for her father mentioning that she was going to meet her school friend. A few weeks later Jessica's dead body was found near a dumping yard.

Investigators were called in to investigate Jessica's death. A preliminary investigation of Jessica's computer and logs revealed some facts that helped the cops trace the killer.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



# Network Forensics




- Network forensics is the capturing, recording, and **analysis of network event** in order to discover the source of security incidents
- Capturing network traffic over a network is simple in theory, but relatively **complex** in practice; because of the large amount of data that flows through a network and the complex nature of the Internet protocols
- **Recording network traffic** involves a lot of resources, which makes it unfeasible to record all the data flowing through the network
- Further, an investigator needs to back up these recorded data to free up recording media and **preserve the data for future analysis**

---

**Network forensics can reveal the following information:**

- Source of security incidents
- The path of intrusion
- The Intrusion techniques an attacker used
- Traces and evidence



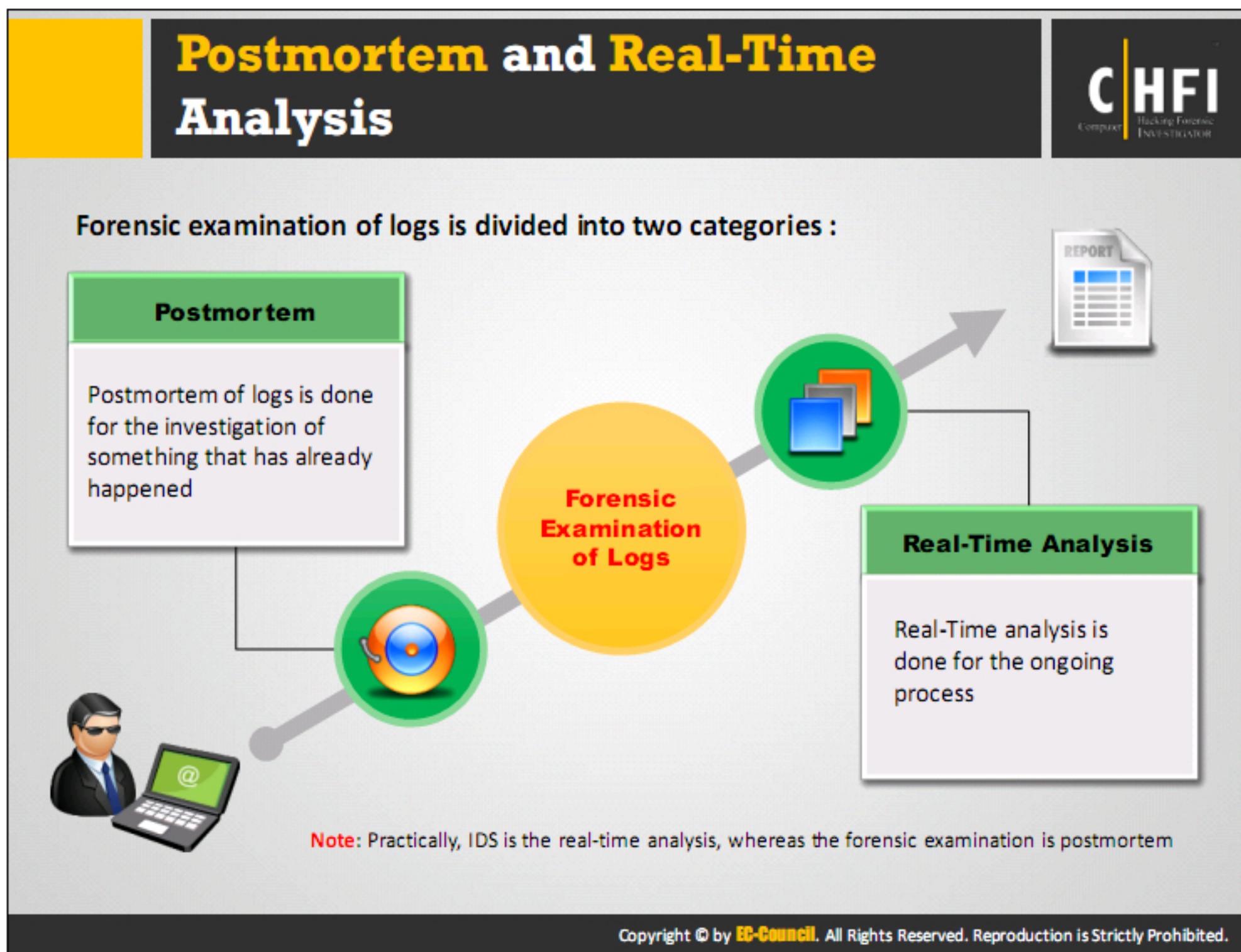
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Network forensics is the implementation of sniffing, recording, acquisition, and analysis of network traffic and event logs to investigate a network security incident. Capturing network traffic over a network is simple in theory, but relatively complex in practice due to many inherent reasons such as the large amount of data flow and complex nature of Internet protocols. Recording network traffic involves a lot of resources. It is often not possible to record all the data flowing through the network due to the large volume. Again, these recorded data need to be backed up to free recording media and for future analysis.

The analysis of recorded data is the most critical and time-consuming task. There are many automated analysis tools for forensic purposes, but they are insufficient, as there is no foolproof method to recognize bogus traffic generated by an attacker from a pool of genuine traffic. Human judgment is also critical because with automated traffic analysis tools, there is always a chance of false positives.

Network forensics is necessary in order to determine the type of attack over a network and to trace the culprit. A proper investigation process is required to produce the evidence recovered during the investigation in the court of law.





Forensic examination of logs has two categories:

## Postmortem

Investigators perform postmortem of logs to detect something that has already occurred in a network/device and determine what it is.

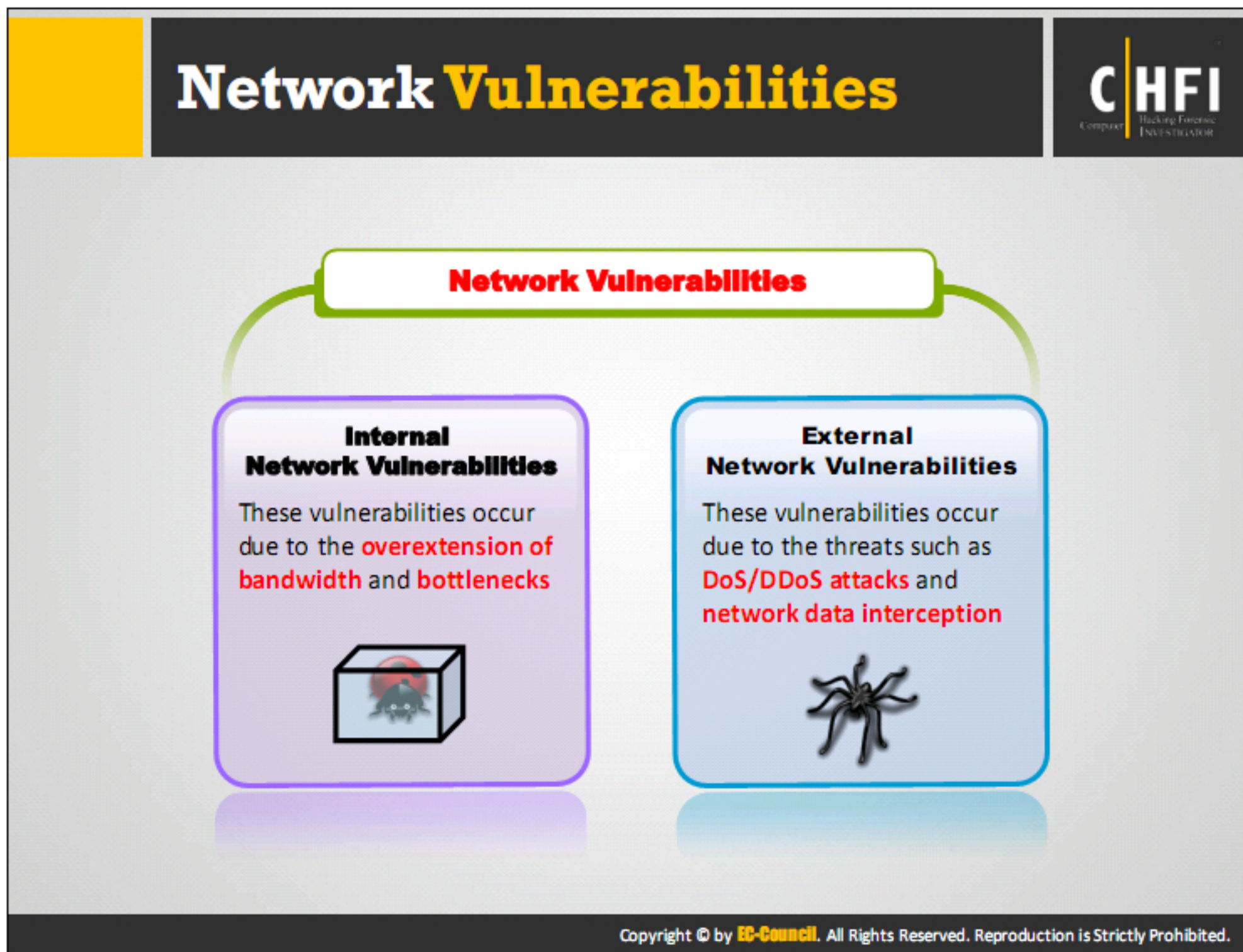
Here, an investigator can go through the log files a number of times to examine and check the flow of previous runs. When compared to real-time analysis, it is an exhaustive process, since the investigators need to examine the attack in detail and give a final report.

## Real-Time Analysis

Real-time analysis is an ongoing process, which returns results simultaneously, so that the system or operators can respond to the attacks immediately.

Real-time analysis is an analysis done for the ongoing process. This analysis will be more effective if the investigators/administrators detect the attack quickly. In this analysis, the investigator can go through the log files only once to evaluate the attack, unlike postmortem analysis.





## Network Vulnerabilities

The massive technological advances in networking have also led to a rapid increase in the complexity and vulnerabilities of networks. The only thing that a user can do is minimize these vulnerabilities, since the complete removal of the vulnerabilities is not possible. There are various internal and external factors that make a network vulnerable.

### Internal network vulnerabilities

Internal network vulnerabilities occur due to the overextension of bandwidth and bottlenecks.

- **Overextension of bandwidth:** Overextension of bandwidth occurs when user need exceeds total resources.
- **Bottlenecks:** Bottlenecks usually occur when user need exceeds resources in particular network sectors.

The network management systems direct these problems and software to the log or other management solutions. System administrators examine these systems and identify the location of network slowdowns. Using this information, they reroute the traffic within the network architecture to increase the speed and functionality of the network.

### External network vulnerabilities

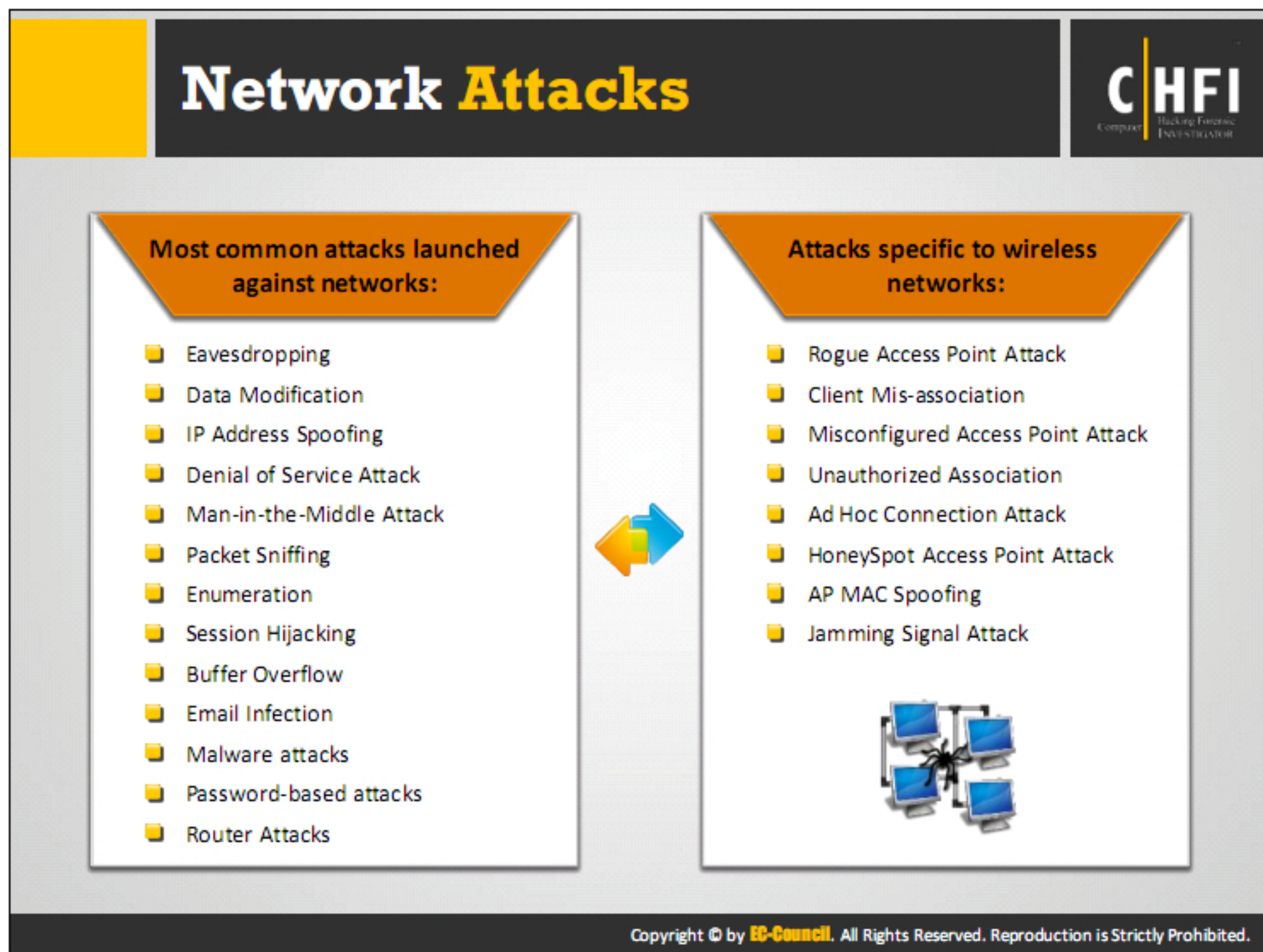
External network vulnerabilities occur due to threats such as DoS/DDoS attacks and network data interception.



DoS and DDoS attacks result from one or numerous attacks. These attacks are responsible for slowing down or disabling the network and are considered as one of the most serious threats that a network faces. To minimize this attack, use network performance monitoring tools that alert the user or the administrator about an attack.

Data interception is a common vulnerability among LANs and WLANs. In this type of attack, an attacker infiltrates a secure session and thus monitors or edits the network data to access or edit the network operation. In order to minimize these attacks, the user or administrator needs to apply user authentication systems and firewalls to restrict unauthorized users from accessing the network.





## Most common attacks against networks:

### Eavesdropping

Eavesdropping is a technique used in intercepting the unsecured connections in order to steal personal information, which is illegal.

### Data Modification

Once the intruder gets access to sensitive information, his or her first step is to alter the data. This problem is referred to as a data modification attack.

### IP Address Spoofing

IP spoofing is a technique used to gain unauthorized access to a computer. Here, the attacker sends messages to the computer with an IP address that indicates the messages are coming from a trusted host.

### Denial of Service (DoS)

In a DoS attack, the attacker floods the target with huge amount of invalid traffic, thereby leading to exhaustion of the resources available on the target. The target then stops responding to further incoming requests, thereby leading to denial of service to the legitimate users.



## **Man-in-the-Middle Attack**

In man-in-the-middle attacks, the attacker makes independent connections with the users/victims and relays messages between them, making them believe that their conversation is direct.

## **Packet Sniffing**

Sniffing refers to the process of capturing traffic flowing through a network, with the aim of gaining sensitive information such as usernames and passwords and using them for illegitimate purposes. In the computer network, packet sniffer captures the network packets. Software tools known as Cain&Able are used to server this purpose.

## **Enumeration**

Enumeration is the process of gathering information about a network that may help in an attacking the network. Attackers usually perform enumeration over the Internet. During enumeration, the following information is collected:

- Topology of the network
- List of live hosts
- Architecture and the kind of traffic (for example, TCP, UDP, IPX)
- Potential vulnerabilities in host systems

## **Session Hijacking**

A session hijacking attack refers to the exploitation of a session-token generation mechanism or token security controls, such that the attacker can establish an unauthorized connection with a target server.

## **Buffer Overflow**

Buffers have data storage capacity. If the data count exceeds the original capacity of a buffer, then buffer overflow occurs. To maintain finite data, it is necessary to develop buffers that can direct additional information when they need. The extra information may overflow into neighboring buffers, destroying or overwriting the legal data.

## **Email Infection**

This attack uses emails as a means to attack a network. Email spamming and other means are used to flood a network and cause a DoS attack.

## **Malware Attacks**

Malware is a kind of malicious code or software designed to damage the system. Attackers try to install the malware on the targeted system; once the user installs it, it damages the system.

## **Password-based attacks**

Password-based attack is a process where the attacker performs numerous login attempts on a system or an application to duplicate the valid login and gain access to it.

## **Router attacks**

It is the process of an attacker attempting to compromise the router and gaining access to it.



## **Attacks specific to wireless networks:**

### **Rogue Access Point Attack**

Attackers or insiders create a backdoor into a trusted network by installing an unsecured access point inside a firewall. They then use any software or hardware access point to perform this kind of attack.

### **Client Mis-association**

The client may connect or associate with an AP outside the legitimate network either intentionally or accidentally. An attacker who can connect to that network intentionally and proceed with malicious activities can misuse this situation. This kind of client mis-association can lead to access control attacks.

### **Misconfigured Access Point Attack**

This attack occurs due to the misconfiguration of the wireless access point. This is the easiest vulnerability the attacker can exploit. Upon successful exploitation, the entire network could be open to vulnerabilities and attacks. One of the means of causing the misconfiguration is to apply default usernames and passwords to use the access point.

### **Unauthorized Association**

In this attack, the attacker takes advantage of soft access points, which are WLAN radios present in some laptops. The attacker can activate these access points in the victim's system through a malicious program and gain access to the network.

### **Ad Hoc Connection Attack**

In an Ad Hoc connection attack, the attacker carries out the attack using an USB adapter or wireless card. In this method, the host connects with an unsecured station to attack a particular station or evade access point security.

### **HoneySpot Access Point Attack**

If multiple WLANs co-exist in the same area, a user can connect to any available network. This kind of multiple WLAN is highly vulnerable to attacks. Normally, when a wireless client switches on, it probes nearby wireless networks for a specific SSID. An attacker takes advantage of this behavior of wireless clients by setting up an unauthorized wireless network using a rogue AP. This AP has high-power (high gain) antennas and uses the same SSID of the target network. Users who regularly connect to multiple WLANs may connect to the rogue AP. These Aps mounted by the attacker are "honeypot" APs. They transmit a stronger beacon signal than the legitimate APs. NICs searching for the strongest available signal may connect to the rogue AP. If an authorized user connects to a honeypot AP, it creates a security vulnerability and reveals sensitive user information such as identity, user name, and password to the attacker.

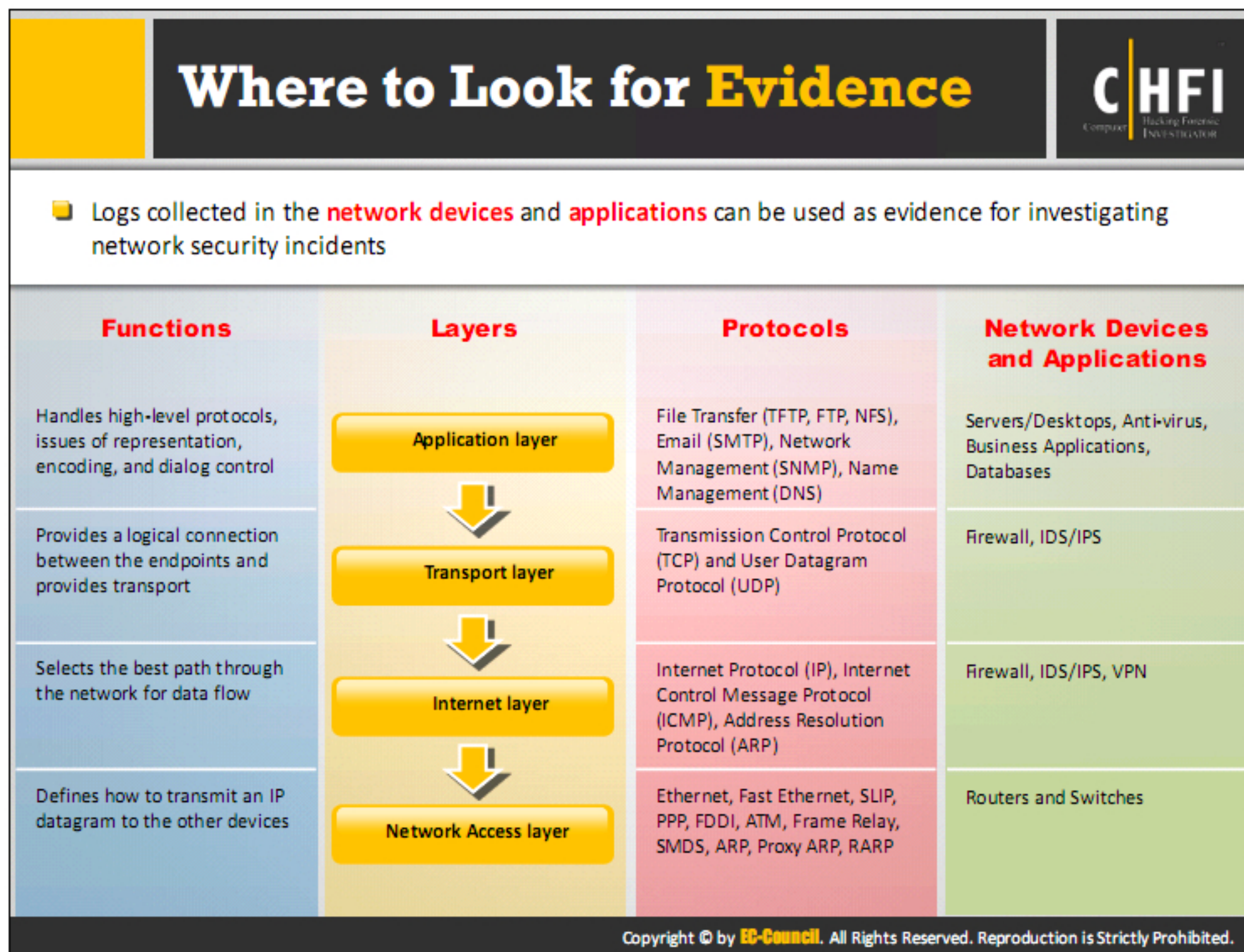
### **AP MAC Spoofing**

Using the MAC spoofing technique, the attacker can reconfigure the MAC address in such a way that it appears as an authorized access point to a host on a trusted network. The tools for carrying out this kind of attack are changemac.sh, SMAC, and Wicontrol.



## Jamming Signal Attack

In this attack, the attacker jams the WiFi signals to stop the all the legitimate traffic from using the access point. The attacker blocks the signals by sending huge amounts of illegitimate traffic to the access point by using certain tools



Logs contain events associated with all the activities performed on a system or a network. Hence, analyzing these logs help investigators trace back the events that have occurred. Logs collected in the network devices and applications serve as evidence for investigators to investigate network security incidents. Therefore, investigators need to have knowledge on network fundamentals, TCP/IP model, and the layers in the model.

Transmission Control Protocol/Internet Protocol (TCP/IP) is a communication protocol used to connect different hosts in the Internet. Every system that sends and receives information has a TCP/IP program, and the TCP/IP program has two layers:

- **Higher Layer:** It manages the information sent and received in the form of small data packets sent over Internet and joins all those packets as a main message.
- **Lower Layer:** It handles the address of every packet so that they all reach the right destination.



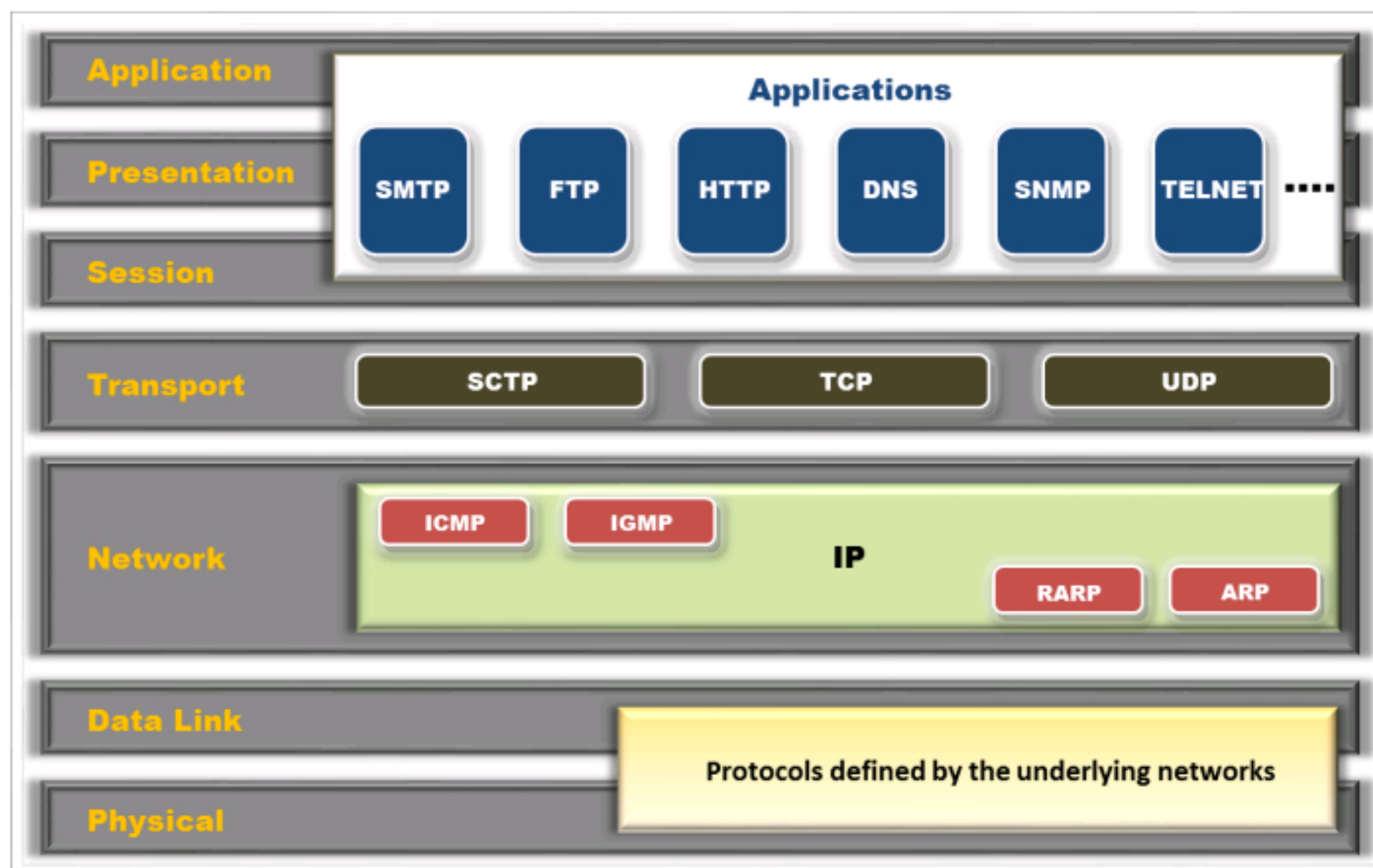


FIGURE 7.1: OSI Model

The OSI 7 Layer model and TCP/IP 4 Layer model are as shown below:

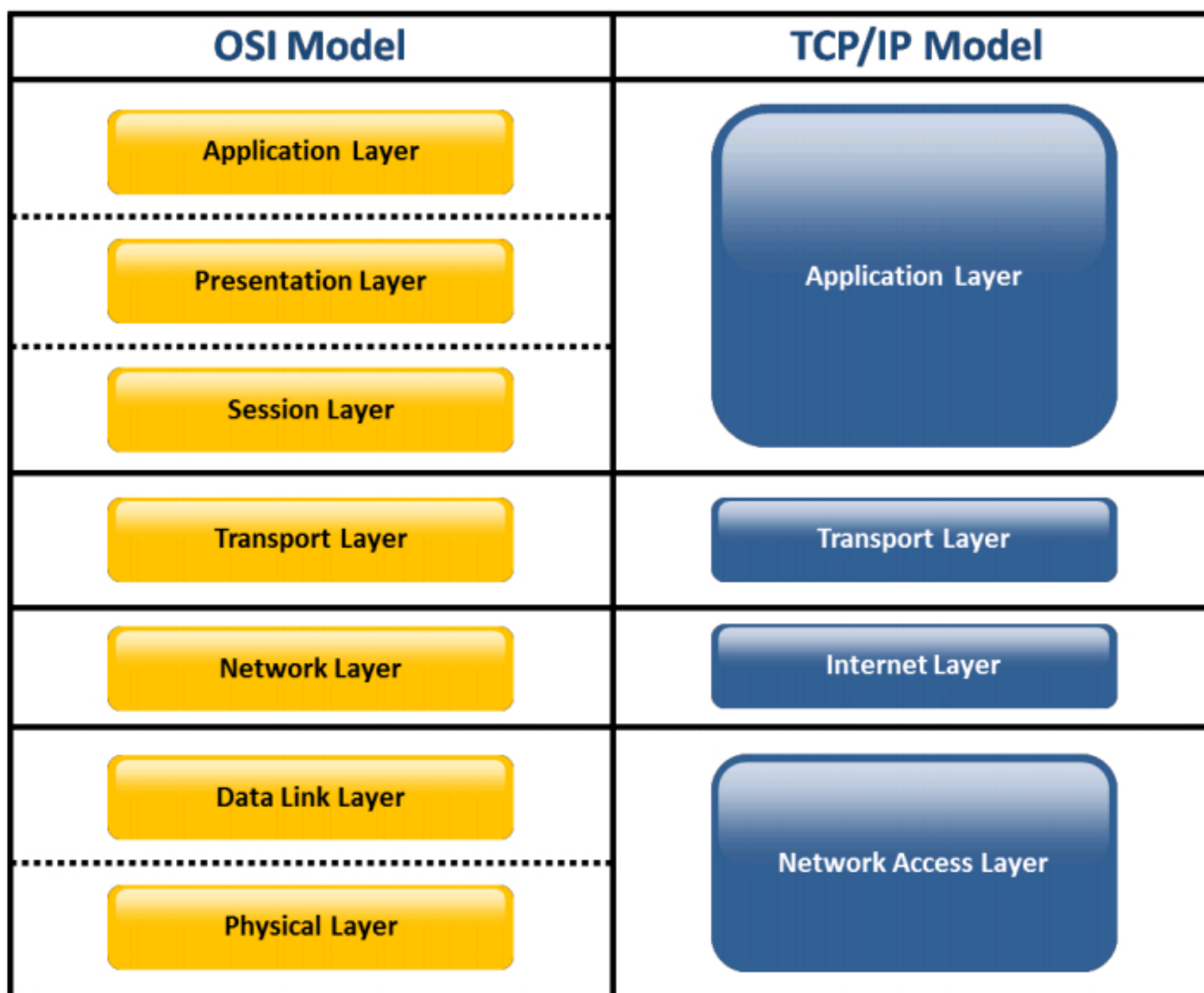


FIGURE 7.2: OSI Model vs. TCP/IP Model



The TCP/IP model and OSI seven-layer models are similar in appearance. As shown in the above figure, the Data Link Layer and Physical Layer of OSI model together form Network Access Layer in TCP/IP model. The Application Layer, Presentation Layer, and Session Layer together form the Application Layer in the TCP/IP Model.

### **Layer 1: Network Access Layer**

This is the lowest layer in the TCP/IP model. This layer defines how to use the network to transfer data. It includes protocols such as Frame Relay, SMDS, Fast Ethernet, SLIP, PPP, FDDI, ATM, Ethernet, ARP, etc., which help the machine deliver the desired data to other hosts in the same network.

### **Layer 2: Internet Layer**

This is the layer above Network Access Layer. It handles the movement of data packet over a network, from source to destination. This layer contains protocols such as Internet Protocol (IP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Internet Group Management Protocol (IGMP), etc. The Internet Protocol (IP) is the main protocol used in this layer.

### **Layer 3: Transport Layer**

Transport Layer is the layer above the Internet Layer. It serves as the backbone for data flow between two devices in a network. The transport layer allows peer entities on the source and destination devices to carry on a communication. This layer uses many protocols, among which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the most widely used.

TCP is preferable in case of reliable connections, while UDP can handle non-reliable connections.

### **Layer 4: Application Layer**

This is the topmost layer of the TCP/IP protocol suite. This layer includes all processes that use the Transport Layer protocols, especially TCP and UDP, to deliver data. This layer contains many protocols, with HTTP, Telnet, FTP, SMTP, NFS, TFTP, SNMP, and DNS being the most widely used ones.



# Log Files as Evidence

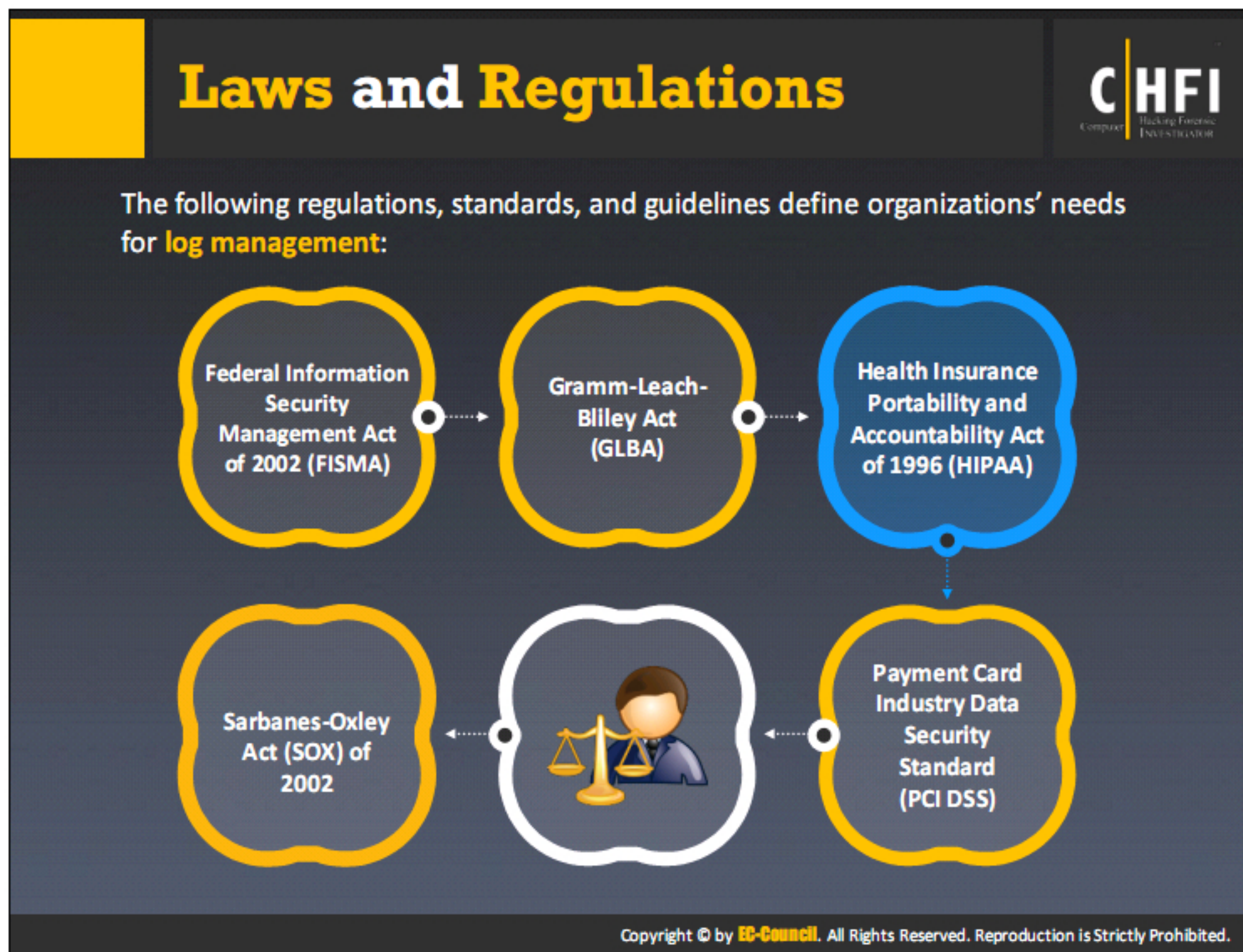


- 1 Log files are the primary records of **user's activity** on **a system** or **a network**
- 2 Investigators use these logs to **recover** any services **altered** and **discover** the source of **illicit activities**
- 3 The basic problem with **logs** is that they can be **altered easily**. An attacker can easily insert false entries into log files
- 4 Computer records are not normally **admissible** as **evidence**; they must meet certain **criteria** to be admitted at all
- 5 The prosecution must present appropriate testimony to show that **logs** are **accurate**, **reliable**, and **fully intact**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

In network forensic investigation, information log files help the investigators lead to the perpetrator. Log files contain valuable data about all the activities performed on the system. Different sources on a network/device produce their respective log files. These sources may be operating systems, IDS, firewall, etc. Comparing and relating the log events help the investigators deduce how the intrusion occurred. The log files collected as evidence need to comply with certain laws to be acceptable in the court; additionally, an expert testimony is required to prove that the log collection and maintenance occurred in the admissible manner.





Source: <https://www.nist.gov>

### **Federal Information Security Management Act of 2002 (FISMA):**

FISMA is the Federal Information Security Management Act of 2002 that states several key security standards and guidelines, as required by Congressional legislation.

FISMA emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets. NIST SP 800-53, Recommended Security Controls for Federal Information Systems, was developed in support of FISMA. 11 NIST SP 800-53 is the primary source of recommended security controls for Federal agencies. It describes several controls related to log management, including the generation, review, protection, and retention of audit records, as well as the actions to be taken because of audit failure.

**Gramm-Leach-Bliley Act (GLBA):** The Gramm-Leach-Bliley Act requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to protect their customers' information against security threats. Log management can be useful in identifying possible security violations and resolving them effectively.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA):** The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes security standards health information. NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, lists HIPAA-related log



management needs. For example, NIST SP 800-66 describes the need to perform regular reviews of audit logs and access reports. Additionally, it specifies that documentation of actions and activities need to be retained for at least six years.

**Sarbanes-Oxley Act (SOX) of 2002:** The Sarbanes-Oxley Act of 2002 (SOX) is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations.

Although SOX applies primarily to financial and accounting practices, it also encompasses the information technology (IT) functions that support these practices. SOX can be supported by reviewing logs regularly to look for signs of security violations, including exploitation, as well as retaining logs and records of log reviews for future review by auditors.

**Payment Card Industry Data Security Standard (PCI DSS):** The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

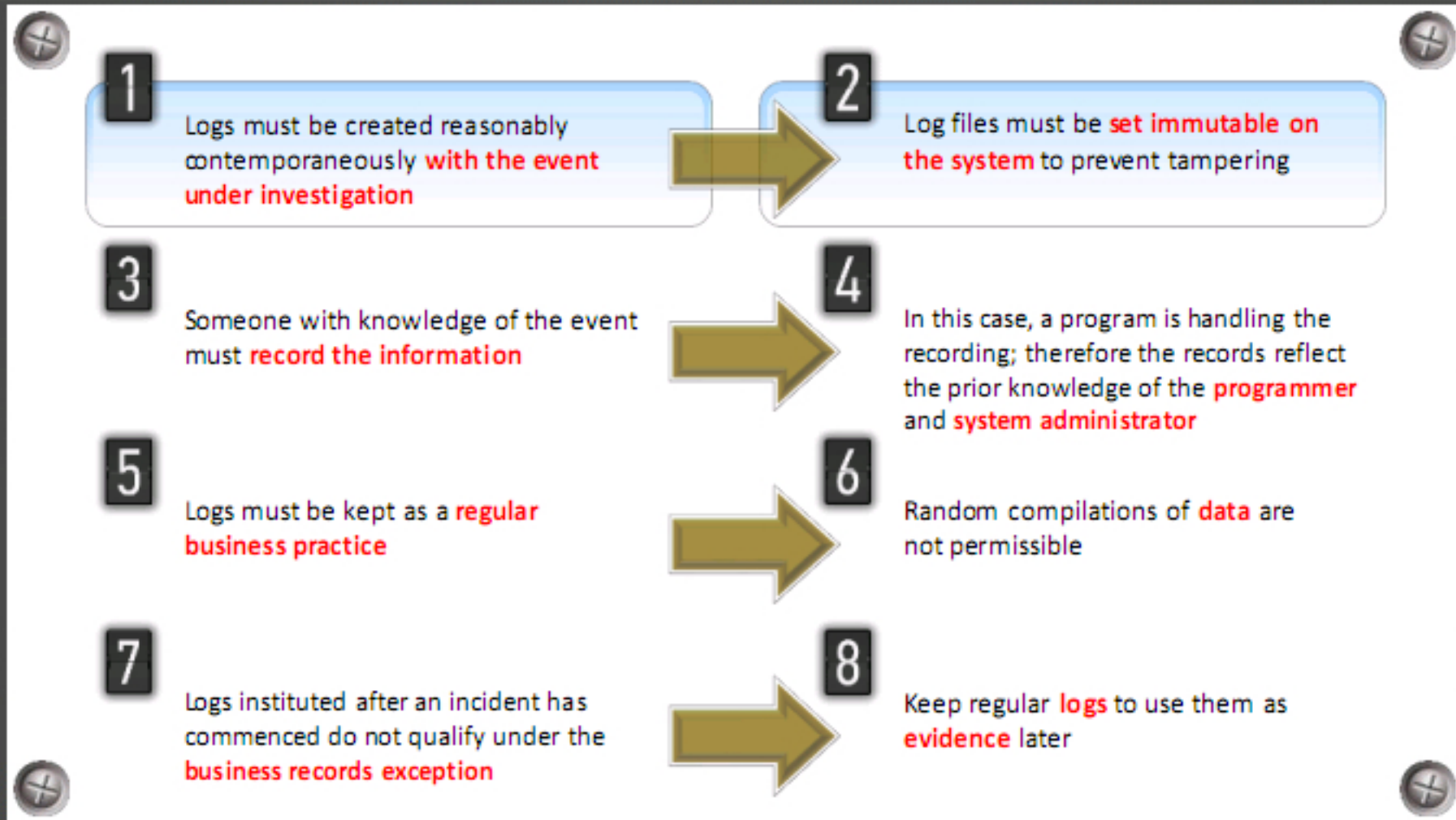
PCI DSS applies to organizations that “store, process, or transmit cardholder data” for credit cards. One of the requirements of PCI DSS is to “track...all access to network resources and cardholder data”.



# Legality of using Logs



Some of the legal issues involved with creating and using logs that organizations and investigators must keep in mind:



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Legality of using Logs (Cont'd)



A "custodian or other qualified witness" must testify to the **accuracy** and **integrity** of the logs. This process is known as authentication

The custodian need not be the programmer who wrote the **logging software**; however, he or she must be able to offer **testimony** on what sort of system is used, where the relevant software came from, how and when the records are produced.



A custodian or other qualified witness must also offer testimony as to the **reliability** and integrity of the **hardware** and **software platform** used, including the logging software

A record of failures or of **security breaches** on the machine creating the logs will tend to impeach the evidence








If an investigator claims that a machine has been penetrated, **log entries** from after that point are inherently suspect

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Legality of using Logs (Cont'd)



1	In a civil lawsuit against alleged hackers, anything in an <b>organization's own records</b> that would tend to exculpate the perpetrators can be used against the organization	
2	An organization's own <b>logging and monitoring software</b> must be made available to the court so that the defense has an opportunity to examine the credibility of the records	
3	If an organization can show that the relevant programs are <b>trade secrets</b> , the organization may be allowed to keep them secret or to disclose them to the defense only under a confidentiality order	
4	The <b>original copies</b> of any files are preferred. A printout of a disk or tape record is considered to be an original copy, unless and until judges and jurors come equipped with computers that have <b>USB or SCSI interfaces</b>	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Records of Regularly Conducted Activity as Evidence



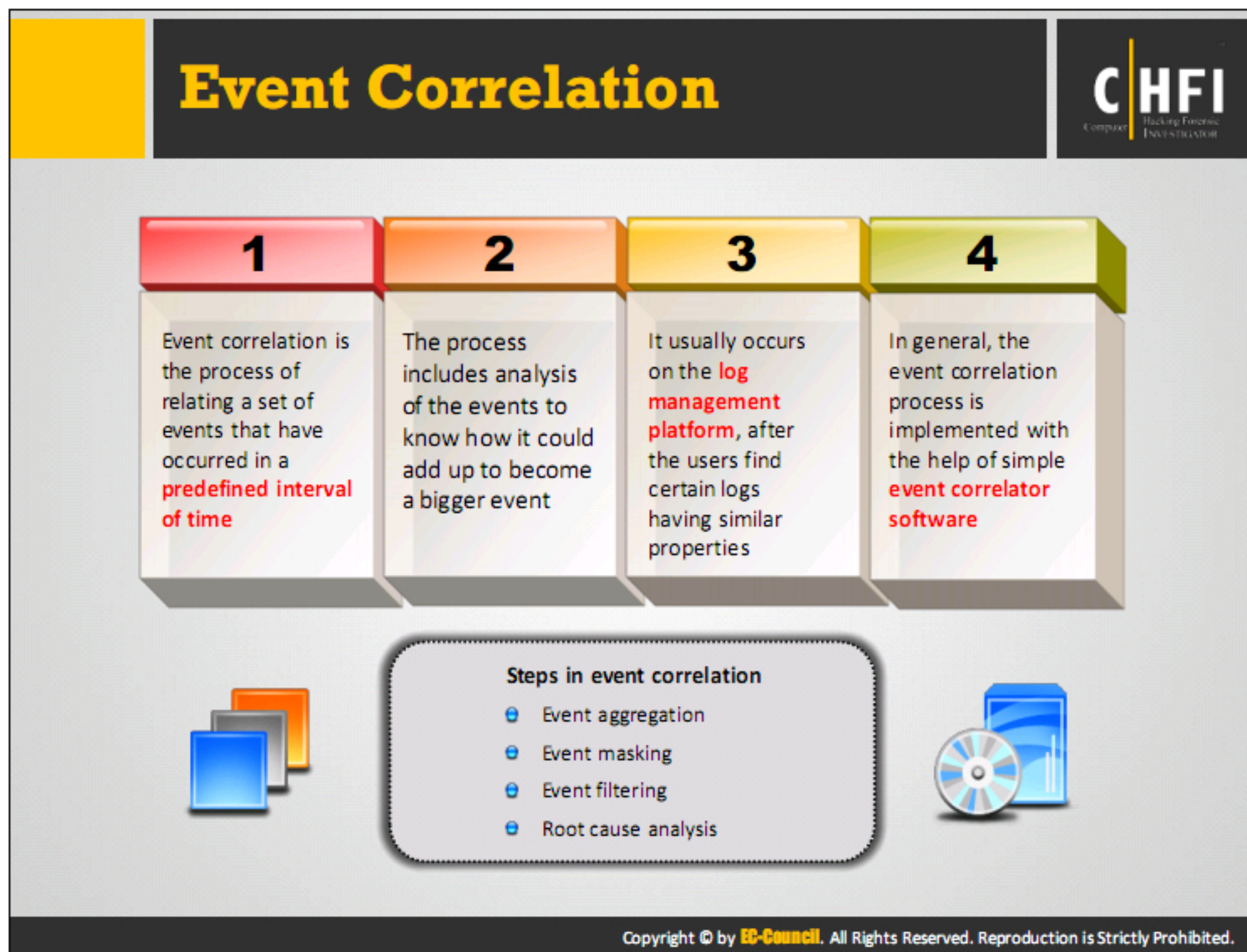


“A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or a statute permitting certification, unless the source of information or the method of circumstances of preparation indicate lack of trustworthiness.”

*Rule 803, Federal Rules of Evidence*

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.





Event correlation is a technique used to assign a new meaning for relating a set of events that occur in a fixed amount of time. This event correlation technique identifies a few events that are important among the large number of events. During the process of event correlation, some new events may occur and delete some existing events from the event stream.

In general, the investigators can perform the event correlation process on a log management platform. Examples of event correlation are as follows:

If a user gets 10 login failure events in 5 minutes, this generates a security attack event.

If both the external and internal temperatures of a device are too high and the event “device is not responding” occurs within 5 seconds, replace them with the event “device down due to overheating.”

Simple event correlator software helps to implement the event correlation process. The event correlator tool collects information about events originating from monitoring tools, managed elements, or the trouble ticket system. This tool processes the relevant events that are important and discards the events that are not relevant while receiving the events.

Event correlation has four different steps, as follows:

### Event aggregation

Event aggregation is also called event de-duplication. It compiles the repeated events to a single event and avoids duplication of the same event.



## **Event masking**

Event masking refers to missing events related to systems that are downstream of a failed system. It avoids the events that cause the system to crash or fail.

## **Event filtering**

Through event filtering, the event correlator filters or discards the irrelevant events.

## **Root cause analysis**

Root cause analysis is the most complex part in event correlation. During a root cause analysis, the event correlator identifies all the devices that became inaccessible due to network failures. Then, the event correlator categorizes the events into symptom events and root cause events. The system considers the events associated with the inaccessible devices as symptom events, and the other non-symptom events as root cause events.



# Types of Event Correlation

**Same-Platform Correlation**

- This correlation method is used when **one common OS** is used throughout the network in an organization
- E.g., an organization running Microsoft Windows OS (any version) for all their servers may be required to **collect event log entries, do trend analysis diagonally**

**Cross-Platform Correlation**

- This correlation method is used when **different OS and network hardware platforms** are used throughout the network in an organization
- E.g., clients may use Microsoft Windows, yet they use a Linux-based firewall and email gateway

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

# Prerequisites of Event Correlation

**Transmission of Data**

- Transmitting data from one security device to another until it **reaches a consolidation point in the automated system**
- To have a secure transmission and to reduce the risk of exposure during data transmission, the data has to be **encrypted and authenticated**

**Normalization**

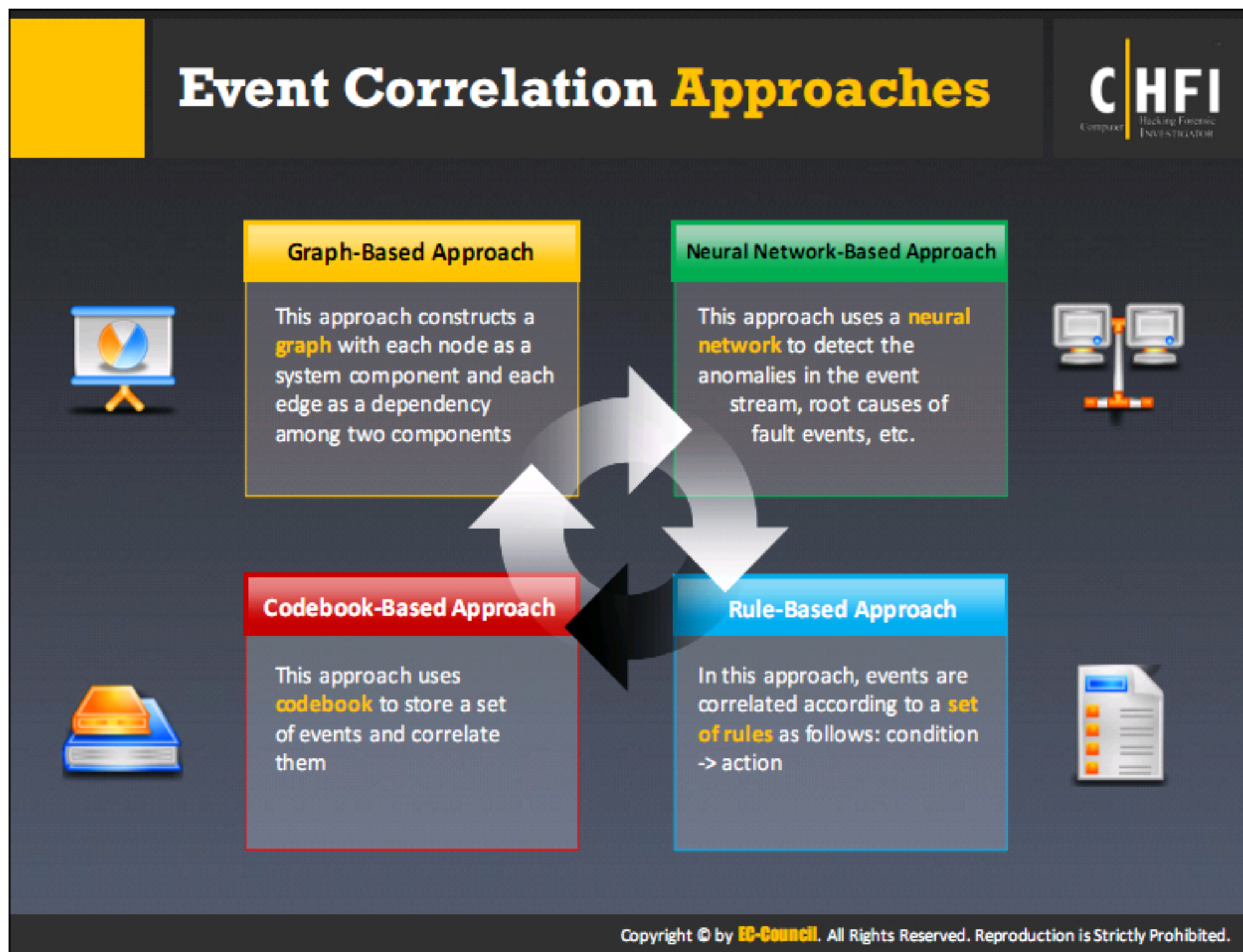
- After the data is gathered, it must be **formatted** again from different log formats to a single or polymorphic log that can be easily inserted into the database

**Data Reduction**

- After collecting the data, repeated data must be **removed** so that the data can be correlated more efficiently
- Removing unnecessary data can be done by **compressing the data, deleting repeated data, filtering** or combining similar events into a single event and sending that to the correlation engine

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.





The graph-based approach finds various dependencies among the system components such as network devices, hosts, services, etc. After detecting the dependencies, this approach constructs the graph with each node as a system component and each edge as a dependency among two components. Thus, when a fault event occurs, the constructed graph is used to detect the possible root cause(s) of fault or failure events.

### Neural Network-Based Approach

This approach uses a neural network to detect the anomalies in the event stream, root causes of fault events, etc.

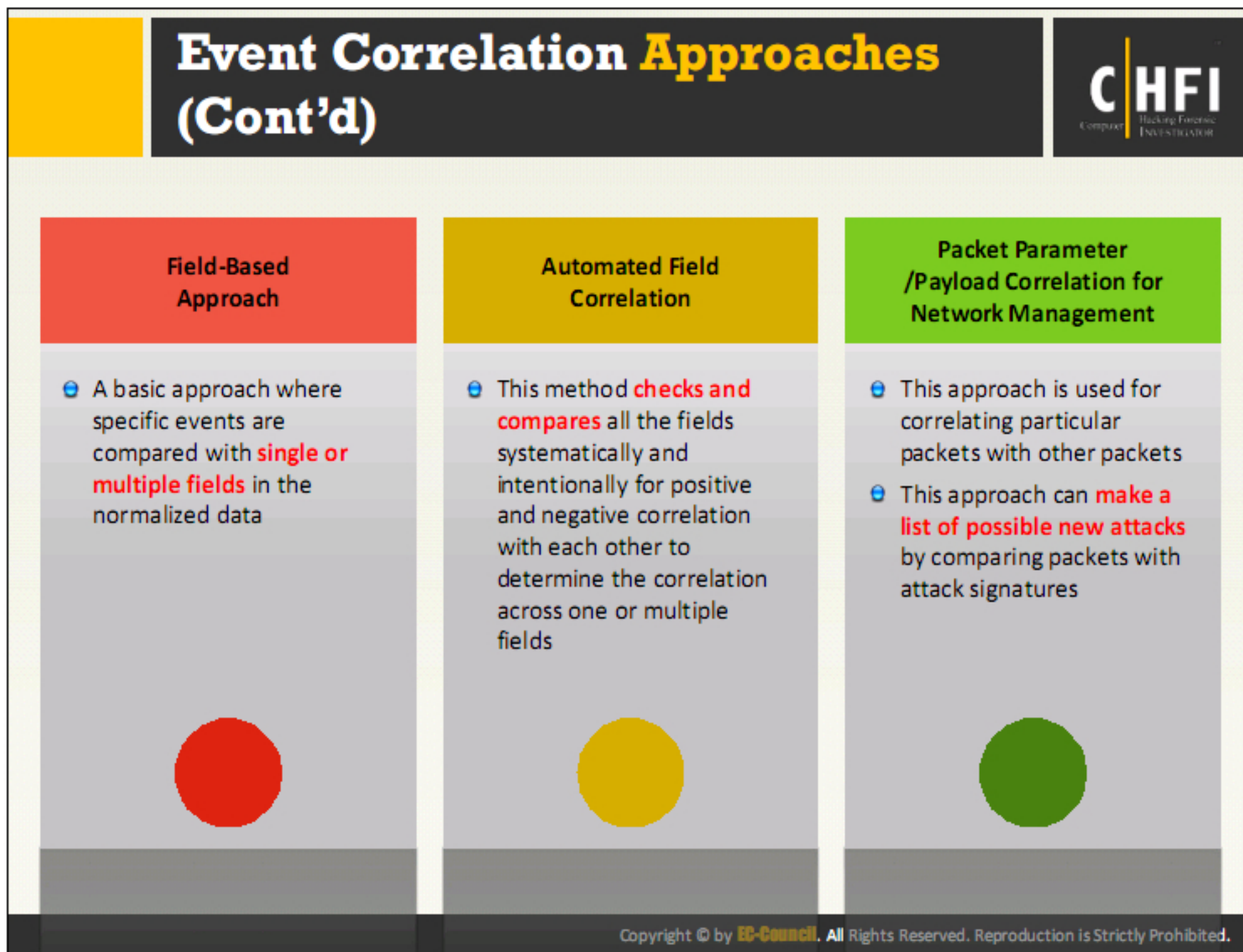
### Codebook-Based Approach

The codebook-based approach is similar to the rule-based approach, which groups all events together. It uses a codebook to store a set of events and correlates them. This approach is executed faster than a rule-based system, as there are fewer comparisons for each event.

### Rule-Based Approach

The rule-based approach correlates events according to a specified set of rules (condition → action). Depending on each test result and the combination of the system events, the rule-processing engine analyzes the data until it reaches the final state.





### Field-Based Approach

This is a basic approach that compares specific events with single or multiple fields in the normalized data.

### Automated Field Correlation


This method checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields.

### Packet Parameter/Payload Correlation for Network Management

This approach helps in correlating particular packets with other packets. This approach can make a list of possible new attacks by comparing packets with attack signatures.



## Event Correlation Approaches (Cont'd)



Profile/Fingerprint-Based Approach	Vulnerability-Based Approach	Open-Port-Based Correlation
<ul style="list-style-type: none"><li>A series of data sets can be gathered from <b>forensic event data</b> such as, isolated OS fingerprints, isolated port scans, finger information, and banner snatching to compare link attack data to other attacker profiles</li><li>This information is used to identify whether any system is a <b>relay</b> or a <b>formerly compromised host</b>, and/or to detect the same hacker from different locations</li></ul>	<ul style="list-style-type: none"><li>This approach is used to map <b>IDS events</b> that target a particular vulnerable host with the help of a vulnerability scanner</li><li>This approach is also used to deduce an attack on a <b>particular host</b> in advance, and it prioritizes attack data so that you can respond to trouble spots quickly</li></ul>	<ul style="list-style-type: none"><li>This approach determines the <b>rate of successful attacks</b> by comparing it with the list of open ports available on the host and that are being attacked</li></ul>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### Profile/Fingerprint-Based Approach

This method helps users identify whether any system is a relay or a formerly compromised host and/or to detect the same hacker from different locations. This approach helps gather a series of data sets from forensic event data, such as isolated OS fingerprints, isolated port scans, finger information, and banner snatching to compare link attack data to other attacker profiles.

### Vulnerability-Based Approach

This approach helps map IDS events that target a particular vulnerable host with the help of a vulnerability scanner.


This approach deduces an attack on a particular host in advance, and it prioritizes attack data in order to respond to the trouble spots quickly.

### Open-Port-Based Correlation

The open-port correlation approach determines the chance of a successful attack by comparing it with the list of open ports available on the host and that are under attack.




## Event Correlation Approaches (Cont'd)




### Bayesian Correlation

This approach is an advanced correlation method that **assumes and predicts what an attacker** can do next after the attack by studying the statistics and probability, and uses only two variables




### Time (Clock Time) or Role-based Approach

This approach is used to monitor **the computers' and computer users' behavior** and provide an alert if something anomalous is found



### Route Correlation

This approach is used to **extract the attack route information** and use that information to single out other attack data



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Bayesian Correlation

This approach is an advanced correlation method that assumes and predicts what a hacker can do next after the attack by studying statistics and probability.

## Time (Clock Time) or Role-Based Approach


This approach eyes the computers' and computer users' behavior and alerts if some anomaly is found.

## Route Correlation

This approach helps extract the attack route information and use that information to single out other attack data.

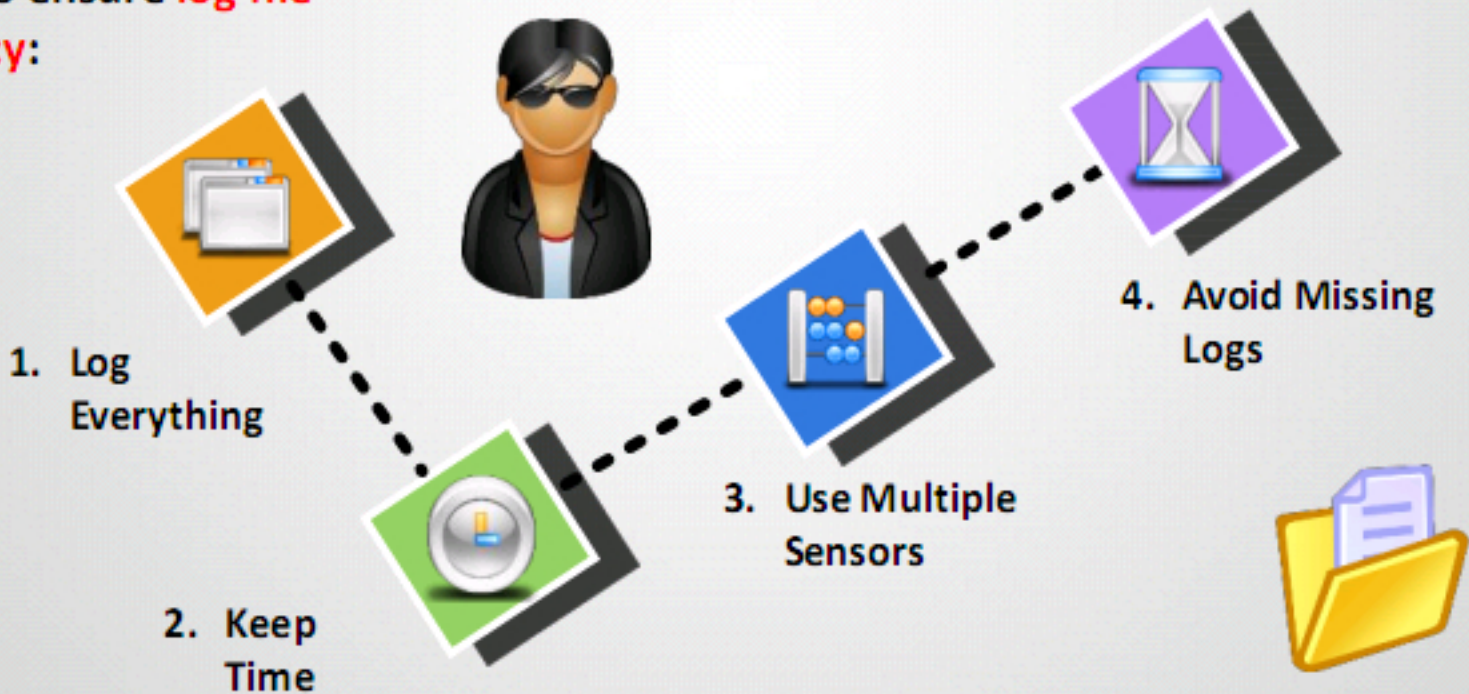


# Ensuring Log File Accuracy



- The reliability of log files directly depends on their **accuracy**
- Accuracy means to **present the log files of investigated system** or server before the court in the same state as available
- Modification to the logs can impact the **validity of the entire log** and subject it to suspicion

**Steps to ensure log file accuracy:**



1. Log Everything
2. Keep Time
3. Use Multiple Sensors
4. Avoid Missing Logs

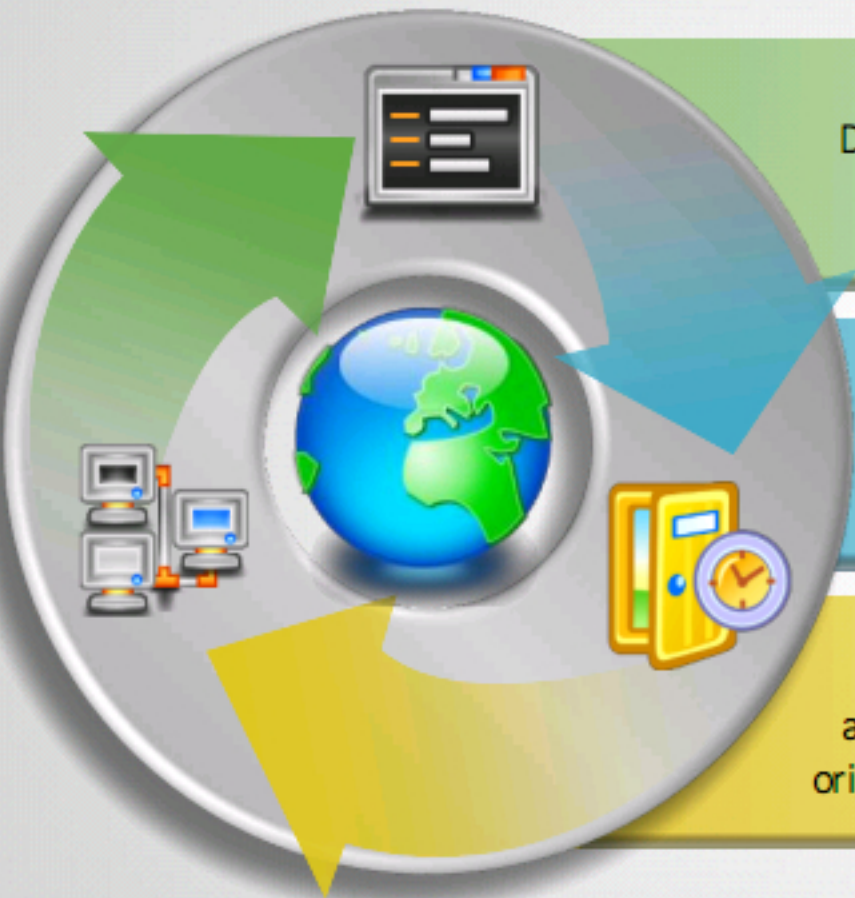
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

During forensic investigation, log files provide a valuable source of evidence. Since these log files act as evidence in court, investigators should ensure that the files are accurate.

Without following certain guidelines while collecting and preserving the log files, they will not be acceptable as valid evidence in the court. Therefore, investigators should follow the above mentioned steps to maintain the log file accuracy.



# Log Everything



Do not consider any field in log files as less important, as every field can **play a major role as evidence**

Network administrators should always **configure the server logs settings** to record every field available

E.g.: Configure IIS logs to record web user information about the Web in order to gather clues about the attack origin either a logged-in user or external system

Consider a defendant who claims a hacker had attacked his system and installed a back-door proxy server on his computer. The attacker then used the back-door proxy to attack other systems. In such a case, how does an investigator prove that the traffic came from a specific user's Web browser or that it was a proxied attack from someone else?


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Configure the web server to log all the fields available. This will help in investigations, as every field shows some information regarding the activity taking place on the system. You cannot predict which field may provide important information and might be evidence.


Logging every possible server activity is a wise decision. For instance, a victim could claim that an intruder had accessed his computer and installed a backdoor proxy server and then started attacking other systems using the same backdoor proxy. In this case, logging every server activity may help investigators in identifying the origin of traffic and the perpetrator of the crime.



# Keeping Time



- With the Windows time service, a network administrator can **synchronize standalone servers** to an external time source
- If you use a domain, the **Time Service** will automatically be synchronized to the **domain controller**



- A network administrator can synchronize a standalone server to an external time source by setting certain registry entries:
  - Key:** HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
  - Setting:** Type
  - Type:** REG\_SZ
  - Value:** NTP
  - Key:** HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\
  - Setting:** NtpServer
  - Type:** REG\_SZ
  - Value:** ntp.xsecurity.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

The time factor is important in a log presented as evidence; therefore, proper and accurate time maintenance is a prerequisite for forensic investigation. It is advisable to synchronize IIS servers using Windows Time service with an external time source. The Windows Time service will automatically synchronize the domain controller in the domain. The standalone server supports synchronization by setting an external source through registry entries, in the following manner:

**Key:** HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\

**Value name:** Type

**Type:** REG\_SZ

**Value data:** NTP

**Key:** HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\

**Value name:** NtpServer

**Type:** REG\_SZ

**Value name:** tock.usno.navy.mil

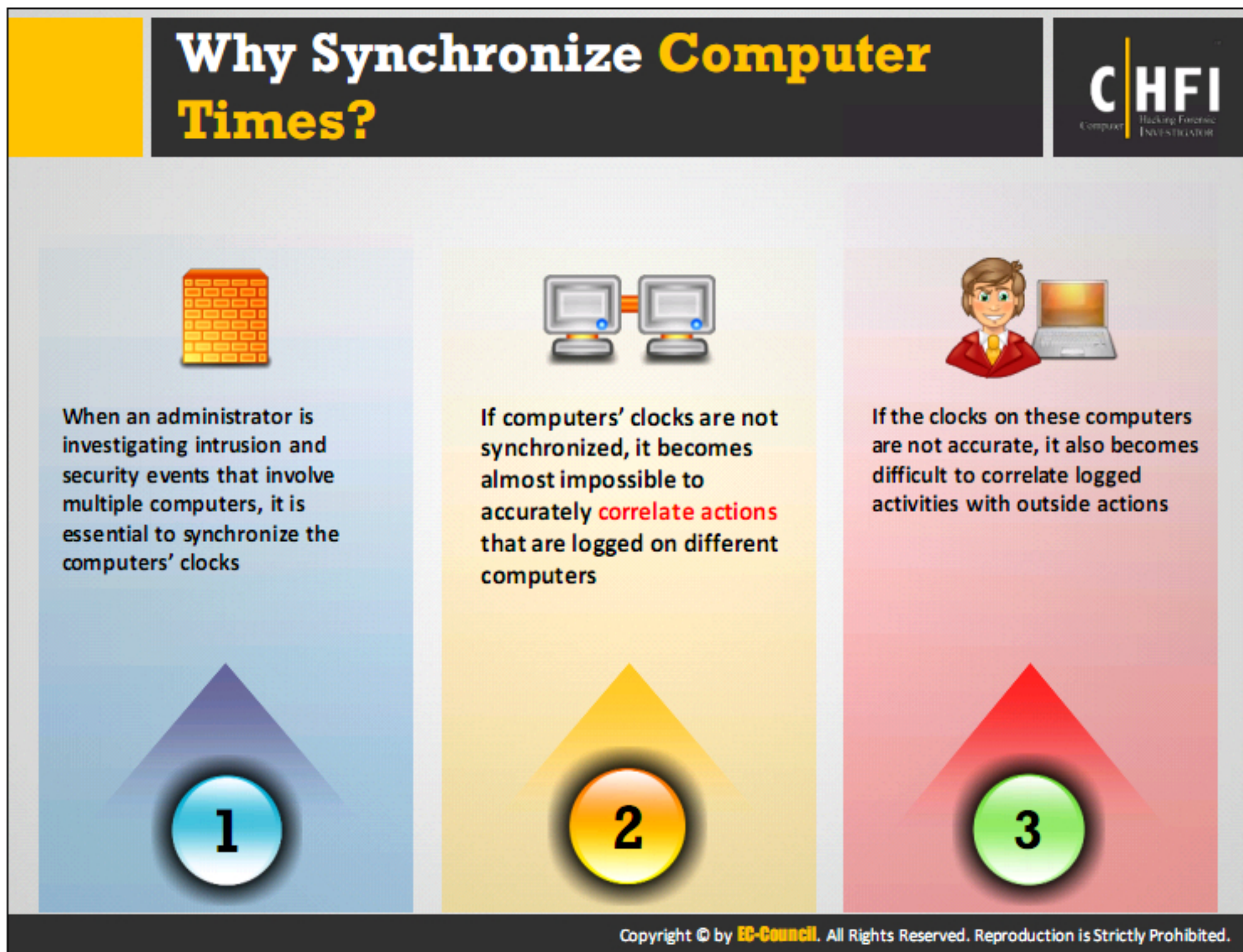
**Key:** HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\

**Value name:** Period

**Type:** REG\_SZ

**Value data:** 24





The most important function of a computer security system is to regularly identify, examine, and analyze the primary log file system as well as check log files generated by intrusion detection systems and firewalls.

Problems faced by the user/organization when the computer times are not in synchronization include the following:


If computers display different times, then it is difficult to match actions correctly on different computers. For example, consider the chat option via any messenger. Two systems with different clocks are communicating, and since the clocks are different, the logs show different times. Now, if an observer checks the log files of both the systems, he or she would face difficulty in reading the conversation.

If the computers connected in the internal (organization) network have the times synchronized but the timings are wrong, the user or an investigator may face difficulty in correlating logged activities with outside actions, such as tracing intrusions.

Sometimes, on a single system, a few applications leave the user puzzled when the time jumps backward or forward. For example, the investigator cannot identify the timings in database systems that are involved in services such as e-commerce transactions or crash recovery.




## What is Network Time Protocol (NTP)?



- It is an Internet standard protocol (built on top of TCP/IP) used to **synchronize the clocks of client computers**
- NTP sends time requests to known servers and obtains **server time stamps**. Using those stamps, it adjusts the client's time

### Features of NTP:

- It is fault tolerant and dynamically auto-configuring
- It synchronizes accuracy up to one millisecond
- It can be used to synchronize all computers in a network
- It uses UTC time
- It is available for every type of computer



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

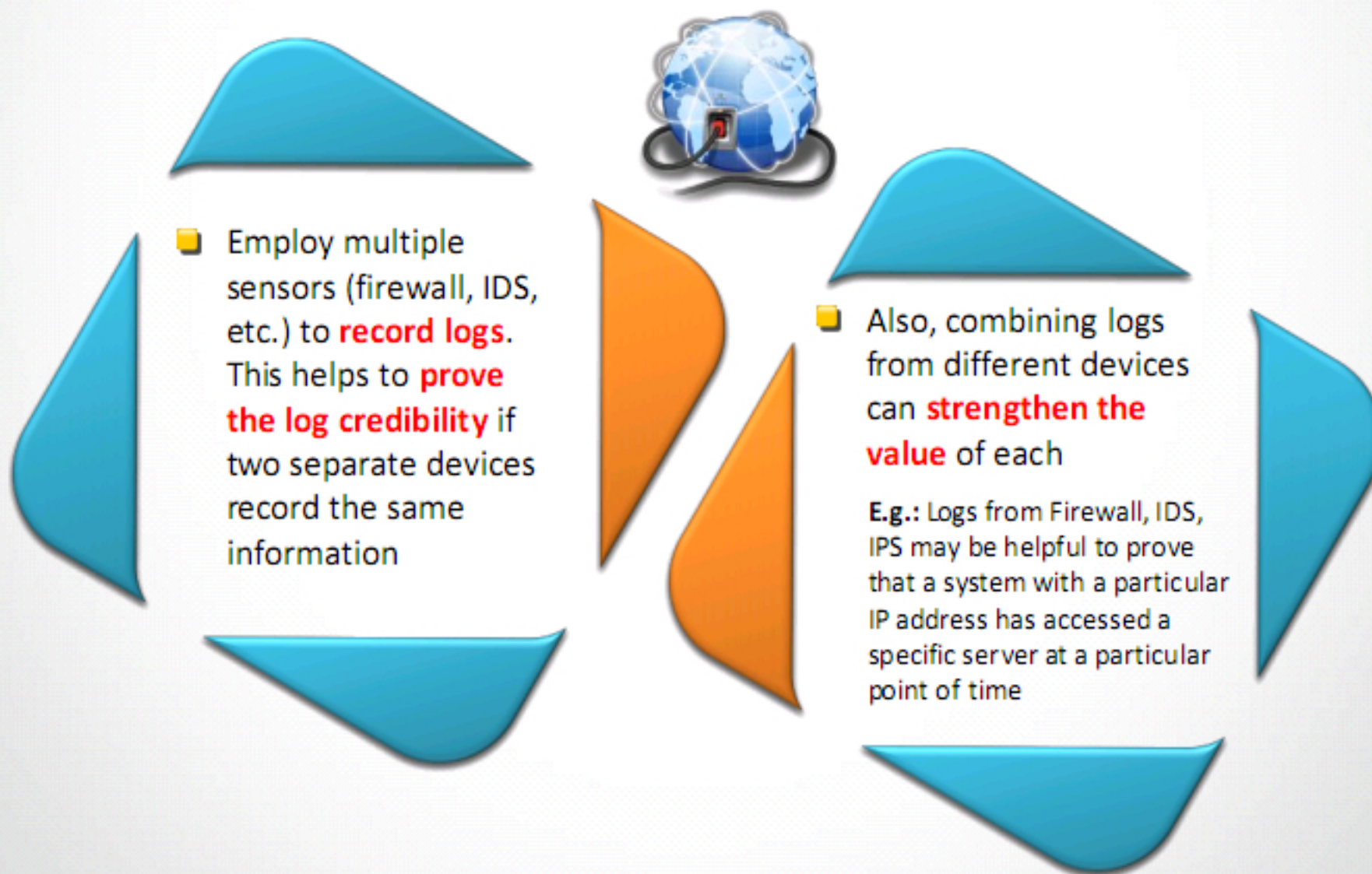
Network Time Protocol (NTP) is a protocol used for synchronizing the time of computers connected to a network. NTP is a standard internet protocol (built on top of TCP/IP) that guarantees perfect synchronization of computer clocks in a computer network to the extent of milliseconds. It runs over packet-switched and variable latency data networks and uses UDP port 123 as its transport layer.

NTP not only synchronizes the clock of a particular system but also synchronizes the client workstation clocks. It runs as a continuous background program on a computer, receiving server timestamps and sending periodic time requests to the server, often working on adjusting the client computer's clock. The features of this protocol are listed below:

- It uses a reference time
- It will choose the most appropriate time when there are many time sources.
- It will try and avoid errors by ignoring inaccurate time sources
- It is highly accessible
- It uses  $2^{32}$  seconds of resolution to choose the most accurate reference time
- It uses measurements from the earlier instances to calculate current time and error, even if the network is not available
- When the network is unavailable, it can estimate the reference time by comparing the previous timings



## Using Multiple Sensors



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

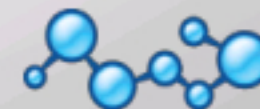
## Avoiding Missing Logs



- When a web server is **offline or powered off**, log files are not created



- When a log file is missing, it is difficult to know if the server was actually offline or powered off, or if the **log file was deleted**



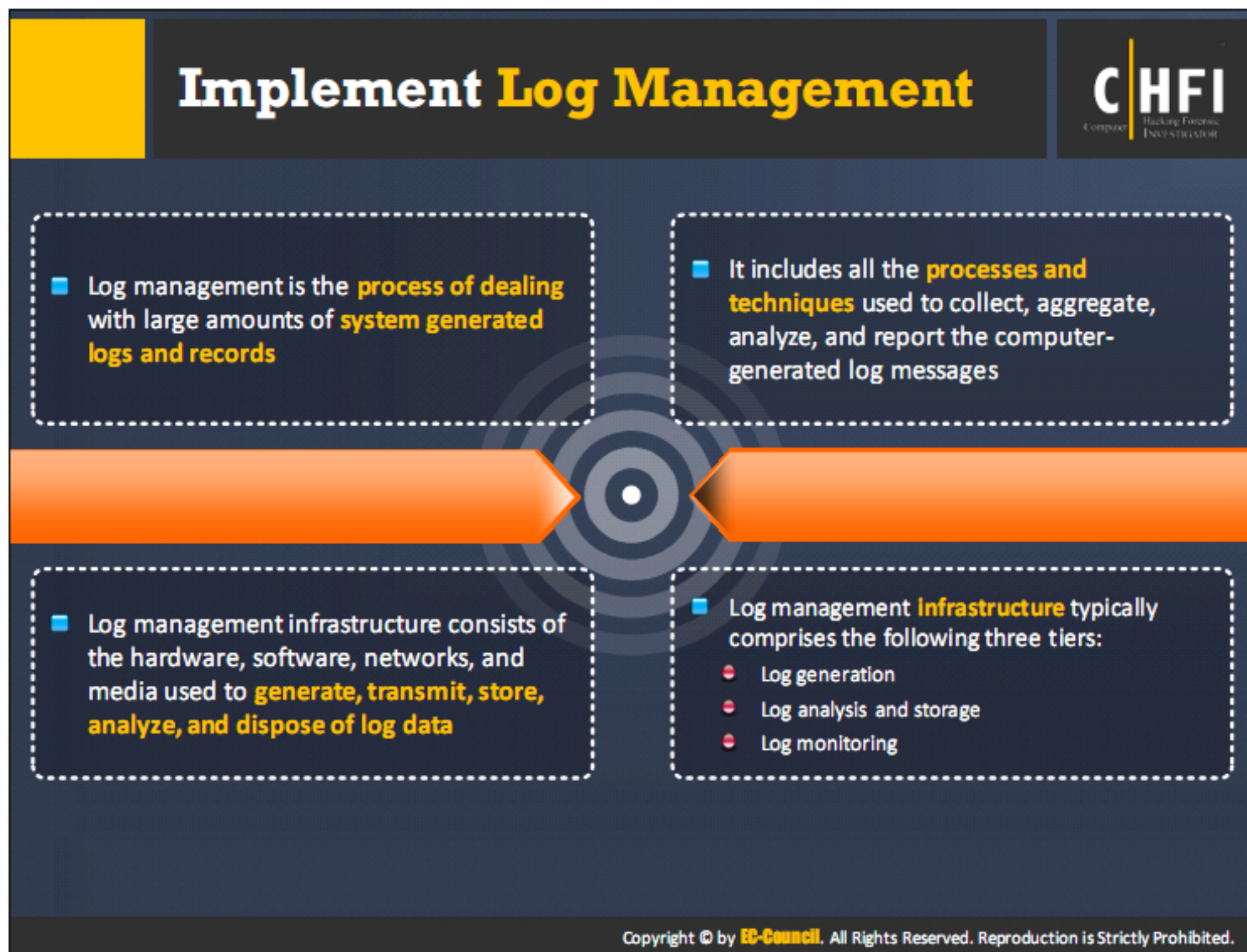
- If the record of hits shows that the server was online and active at the time that **log file data is missing**, the administrator knows that the missing log file might have been deleted

- To combat this problem, an administrator can **schedule a few hits to the server** using a scheduling tool and then keep a log of the outcomes of these hits to determine when the server was active



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.





The records of events taking place in the organization's system and network are logs. A log is a collection of entries, and every entry includes detailed information about all events that occurred within the network. With the increase of workstations, network servers, and other computing services, the volume and variety of logs have also increased. To overcome this problem, log management is necessary.

A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose off the log data.

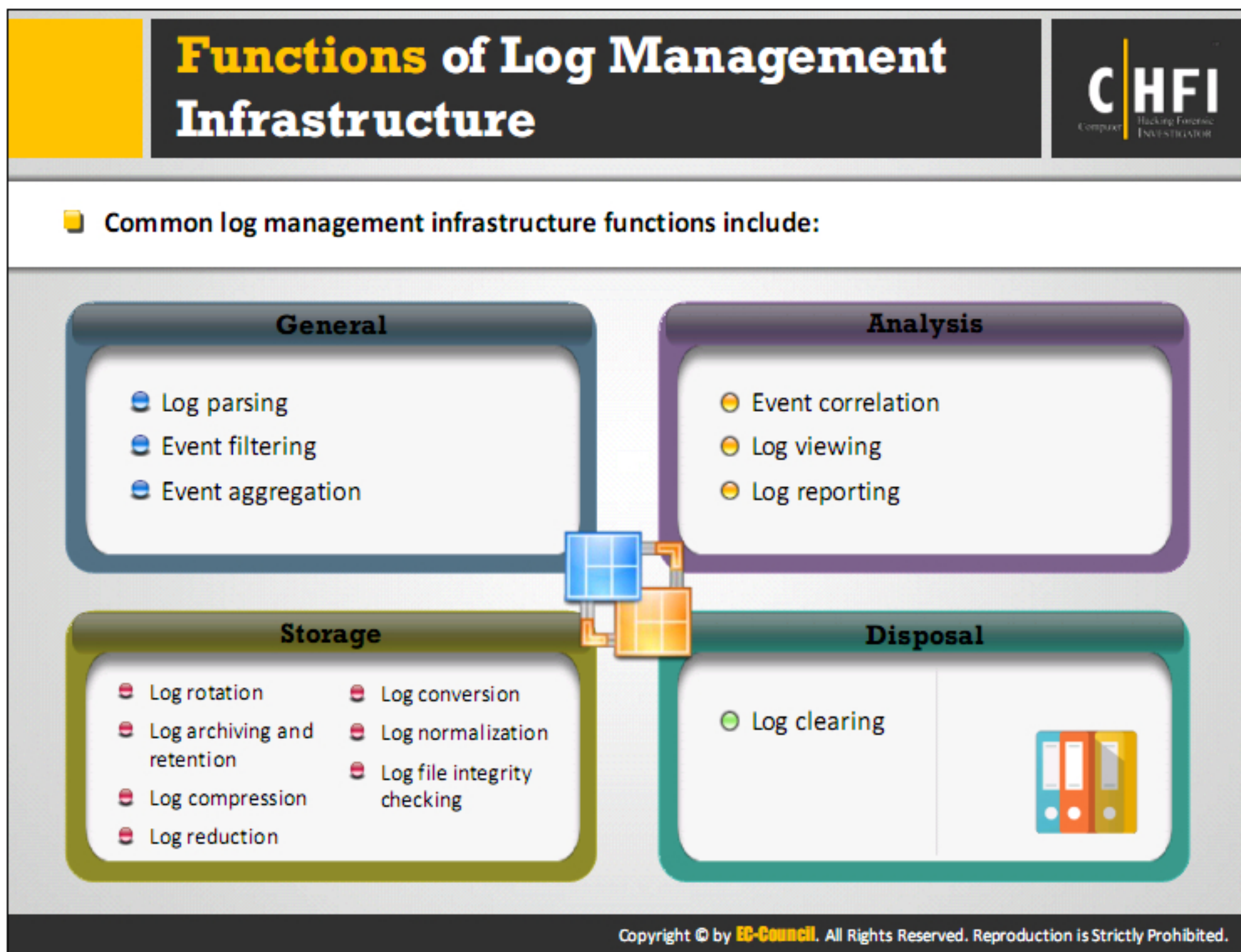
A log management infrastructure typically comprises the following three tiers:

**Log Generation:** The first tier of the log management infrastructure includes hosts that generate log data. Log data can be made available for the log server in the second tier through two means. First, hosts run a log client service or application that makes log data available to the log server through the network. Secondly, the host allows the servers to authenticate and retrieve copies of the log files to the server.

**Log Analysis and Storage:** The second tier consists of log servers that receive log data or copies of log data from the hosts. Log data are transferred from the host to the server in or almost in real time. Data also travel in batches based on a schedule or on the amount of log data waiting. Log servers or on separate database servers store the log data.

**Log Monitoring:** The third tier of the log management infrastructure contains consoles that monitor and review log data. These consoles also review the results of the automated analysis and generate reports.





A log management system performs the following functions:


- **Log parsing:** Log parsing refers to extracting data from a log so that the parsed values can be used as input for another logging process.
- **Event filtering:** Event filtering is the suppression of log entries through analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest.
- **Event aggregation:** Event aggregation is the process where similar entries are consolidated into a single entry containing a count of the number of occurrences of the event.
- **Log rotation:** Log rotation closes a log file and opens a new log file on completion of the first file. It is performed according to a schedule (e.g., hourly, daily, weekly) or when a log file reaches a certain size.
- **Log archival and retention:** Log archival refers to retaining logs for an extended time period, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server. Investigators need to preserve the logs, to meet legal and/or regulatory requirements. Log retention is archiving logs on a regular basis as part of the standard operational activities.




- **Log compression:** Log compression is the process of storing a log file in a way that reduces the amount of storage space needed for the file without altering the meaning of its contents. It is often performed when logs are rotated or archived.
- **Log reduction:** Log reduction is removing unneeded entries from a log to create a new log that is smaller. A similar process is event reduction, which removes unneeded data fields from all log entries.
- **Log conversion:** Log conversion is parsing a log in one format and storing its entries in a second format. For example, conversion could take data from a log stored in a database and save it in an XML format in a text file.
- **Log normalization:** In log normalization, each log data field is converted to a particular data representation and categorized consistently. One of the most common uses of normalization is storing dates and times in a single format.
- **Log file integrity checking:** Log file integrity checking involves the calculation of a message digest for each file and storing the message digest securely to ensure detection of the changes made to the archived logs.
- **Event correlation:** Event correlation is determining relationships between two or more log entries. The most common form of event correlation is rule-based correlation, which matches multiple log entries from a single source or multiple sources based on the logged values, such as timestamps, IP addresses, and event types.
- **Log viewing:** Log viewing displays log entries in a human-readable format. Most log generators offer some sort of log viewing capability; third-party log viewing utilities are also available. Some log viewers provide filtering and aggregation capabilities.
- **Log reporting:** Log reporting is displaying the results of log analysis. It is often performed to summarize significant activity over a particular period of time or to record the detailed information related to a particular event or series of events.
- **Log clearing:** Log clearing removes all entries from a log that precede a certain date and time. It is often performed to remove old log data that is no longer needed on a system because it is not of importance or because it has been archived.




## Challenges in Log Management






- Potential problems with the gathering of logs because of their **variety and dominant occurrence**



- Compromise of confidentiality, integrity, and availability of the logs is often **intentional or accidental**



- People performing log analysis have **no formal training** and often deprived of proper support

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

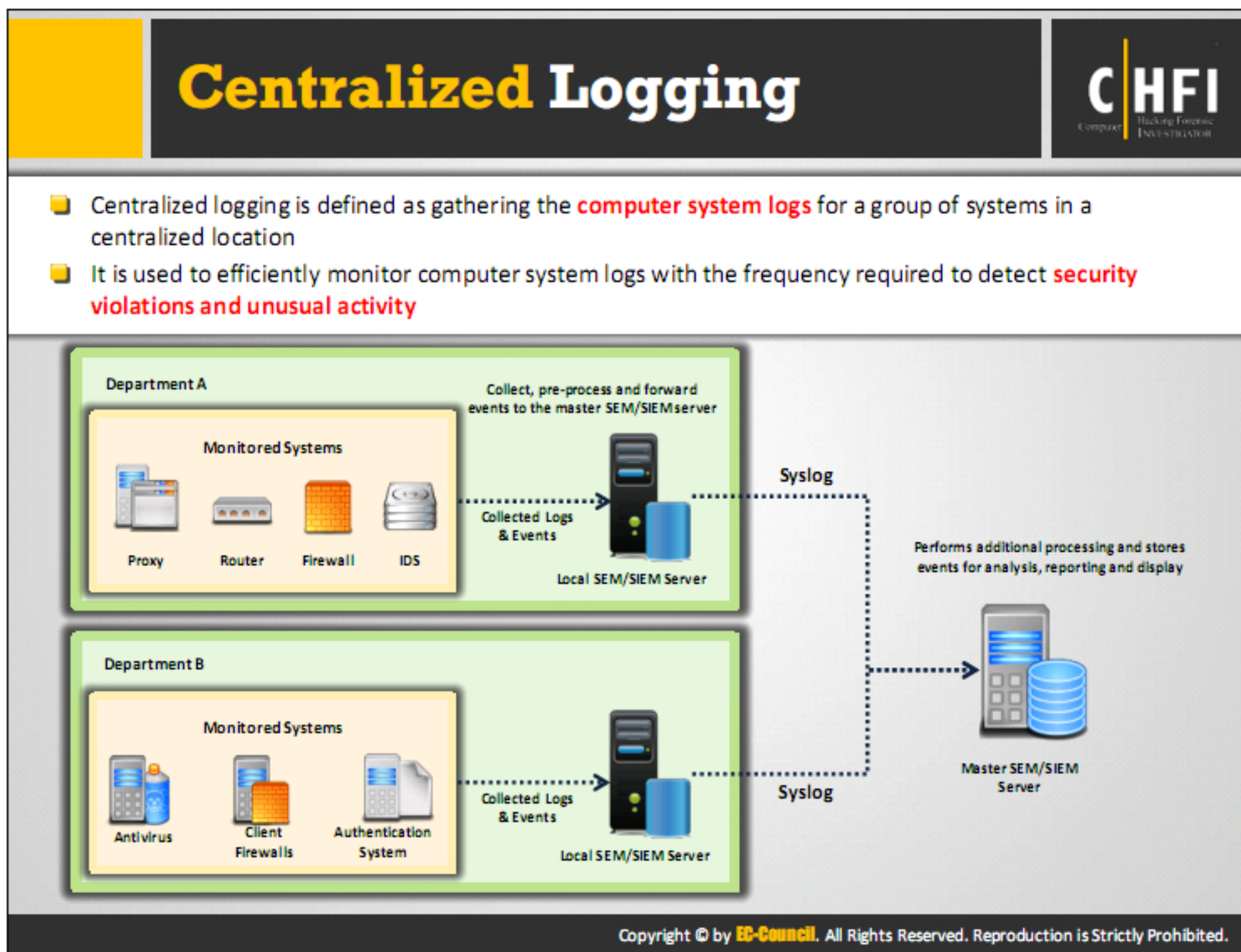
There are three major concerns regarding the log management. The first one is the creation and storage of logs; the second is protecting the logs; and the third is analyzing logs. They are the most important challenges of the log management that will have an impact on the forensic investigation.

- **Log creation and storage:** There are huge amounts of logs generated from several system resources. Due to their large size, the question of log storage is challenging. The log format is another thing that makes it difficult to manage the logs since different devices and log-monitoring systems produce logs with different formats.
- **Log protection:** Log protection and availability are the foremost considerations in an investigation since the evidence it holds is very valuable. If investigators do not properly handle the logs during forensic examinations, the files lose their integrity and become invalid as evidences.
- **Log Analysis:** Logs are very important in an investigation; therefore, ensuring proper log analysis is necessary. However, log analysis is not a high priority job for the administrators. Log analysis is the last thing to do for the administrators because it takes place after an incident occurs. Therefore, there is a lack of tools and skillful professionals for log analysis, making it a major drawback.









Centralized logging is defined as a gathering of the computer system logs for a group of systems in a centralized location. All network logs are stored on a centralized server or computer, which helps administrators perform easy backup and retrieval. It allows the administrator to check logs on each system on a regular basis. It is used to efficiently monitor computer system logs with the frequency required to detect security violations and unusual activity.

Centralized logging offers the following:

- Trail can be reviewed if the client machine is compromised
- It allows for a central place to run log checking scripts
- It is highly secure with no other
- Packet is filtered/firewalled to allow only approved machines
- Logs can be sent to any email address for daily analysis
- It has suitable backup and restoration ability

All security event management (SEM) systems provide solutions for security events related to collection, processing, and storage. Dedicated SEM servers are used to centralize the functions so that security events are managed centrally.



Using a centralized system has many benefits, such as providing centralized backups, and will also be beneficial in detecting and analyzing events. Servers are maintained at two levels:

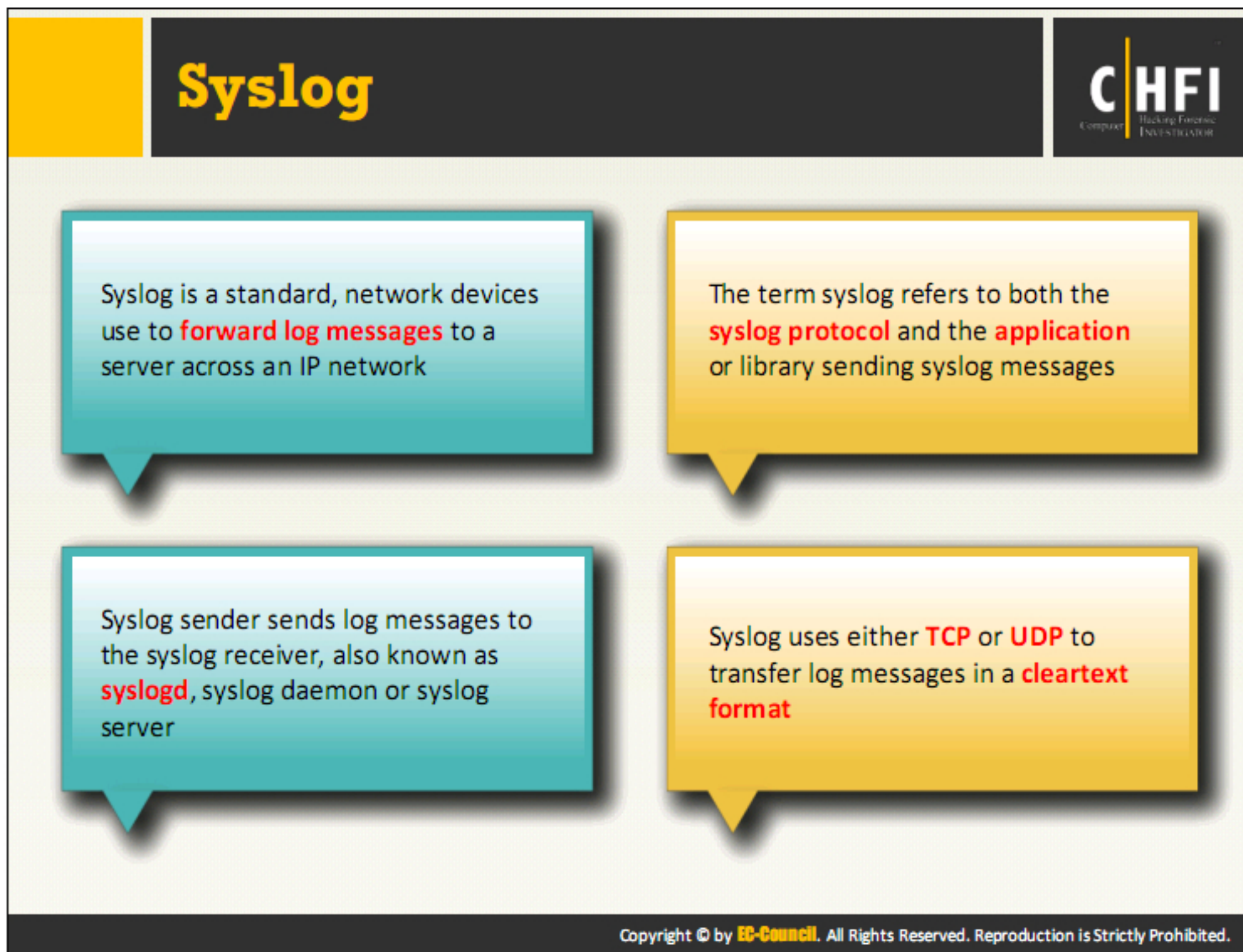
1. Local SEM server
2. Master SEM server

The local SEM server collects, processes, and queues all the events and forwards further tasks to the master SEM.

The master SEM server executes the subsequent functions of processing and storing the security events for analysis, reporting, and display. Usually, highly configured systems are needed for the master SEM because it needs a large storage capacity.

Depending on the storage space available on the central SEM server, security events are stored for periods ranging from a few weeks to months.





Syslog is a de-facto standard for logging system events. It is a client/server protocol used for forwarding log messages across an IP network to the syslog receiver. This syslog receiver is also called as syslog server, syslog daemons, or syslogd. The term “syslog” refers to both the syslog protocol and the application or library sending syslog messages. In general, the syslog is used to manage and monitor computer system and security auditing.

Syslog uses either TCP or UDP to transfer messages. The log messages are sent in a clear text format. Different devices and receivers support syslog across multiple platforms.

## Syslog in Unix-like Systems

Source: <http://www.cs.umsl.edu>

Syslog is a comprehensive logging system that manages information created by the kernel and system utilities. In a UNIX-like system, it is the heart of Linux logging. The syslog function sends messages to the system logger. It is controlled through the configuration file `/etc/syslog.conf`. It sorts the messages according to the sources and routes them to various destinations thereby performing several functions, such as the following:

- Sends a message to syslogd
- Logs it in a suitable system log
- Writes it to the system console
- Forwards it to a list of users



The syslog facility is based on two key elements:

- `/etc/syslogd` (the daemon)
- `/etc/syslog.conf` configuration file

There are three parts of syslog:

### 1. **syslogd**

- Logging daemon, along with its config file `/etc/syslog.conf`
- Starts at boot time and runs continuously
- Reads and forwards system messages to appropriate log files and/or users
- Programs write entries to `/dev/log` or `/var/run/log`, which can be a socket, a named pipe, or a STREAMS module
- On Solaris, the STREAMS log driver is `/dev/log`
- Syslogd reads messages from file, consults its configuration file, and dispatches message to appropriate destination
- Logs a mark (timestamps) message every 20 minutes at priority LOG\_INFO to the facility which is identified as a mark in the syslog.conf file
- On some systems, syslogd may also read kernel messages from the device `/dev/klog`
- Writes its process ID to the file `/etc/syslog.pid`:
- Makes it easy to send signals to the syslogd from a script
- Restart syslogd by
  - `kill -HUP '/bin/cat /etc/syslog.pid'`
- Compressing or rotating a log file opened by syslogd has unpredictable results
- Controlled by the file `/etc/syslog.conf`
  - Uses format:
  - `selector<TAB>action`
  - Example: `user.err /var/adm/messages`
- Syslogd produces time stamp messages that are logged if the facility mark appears in syslog.conf to specify a destination for them

2. **openlog**: Initializes logging using the specified facility name

3. **logger**: Adds **entries** to system log

### **Advantages of Centralized Syslog Server:**

In a centralized syslogging setup, a common server receives all syslog messages and logs from all computer systems connected to the network. It receives syslog messages and logs from all




UNIX servers; Windows servers; and network devices such as routers, switches, hubs, firewall, etc.

There are many advantages of centralized syslogging, as follows:

- The central syslog is kept on a different segment for storage security.
- A hacker will find it difficult to delete the logs.
- Log messages allow co-relation of attacks across different platforms.
- It has an easy backup policy.
- Tools like Swatch generate real-time alerts, which help to continuously monitor the log files.



## IIS Centralized Binary Logging



- Centralized binary logging is a process in which many websites write **binary and unformatted log data** to a single log file
- An administrator needs to use a parsing tool to view and analyze the data. The files have the extension .ibl, which stands for the Internet binary log
- It is a server property, so all websites on that server **write log data** to the central log file
- It decreases the amount of system resources that are consumed during logging, therefore increasing performance and scalability

**Fields that are included in the centralized binary log file format:**

Date	Server IP address	Server IP address
Time	Server port	Server port
Client IP address	Method	Method
User name	URI stem	URI stem
Site ID	URI query	URI query
Server name	Protocol status	Protocol status

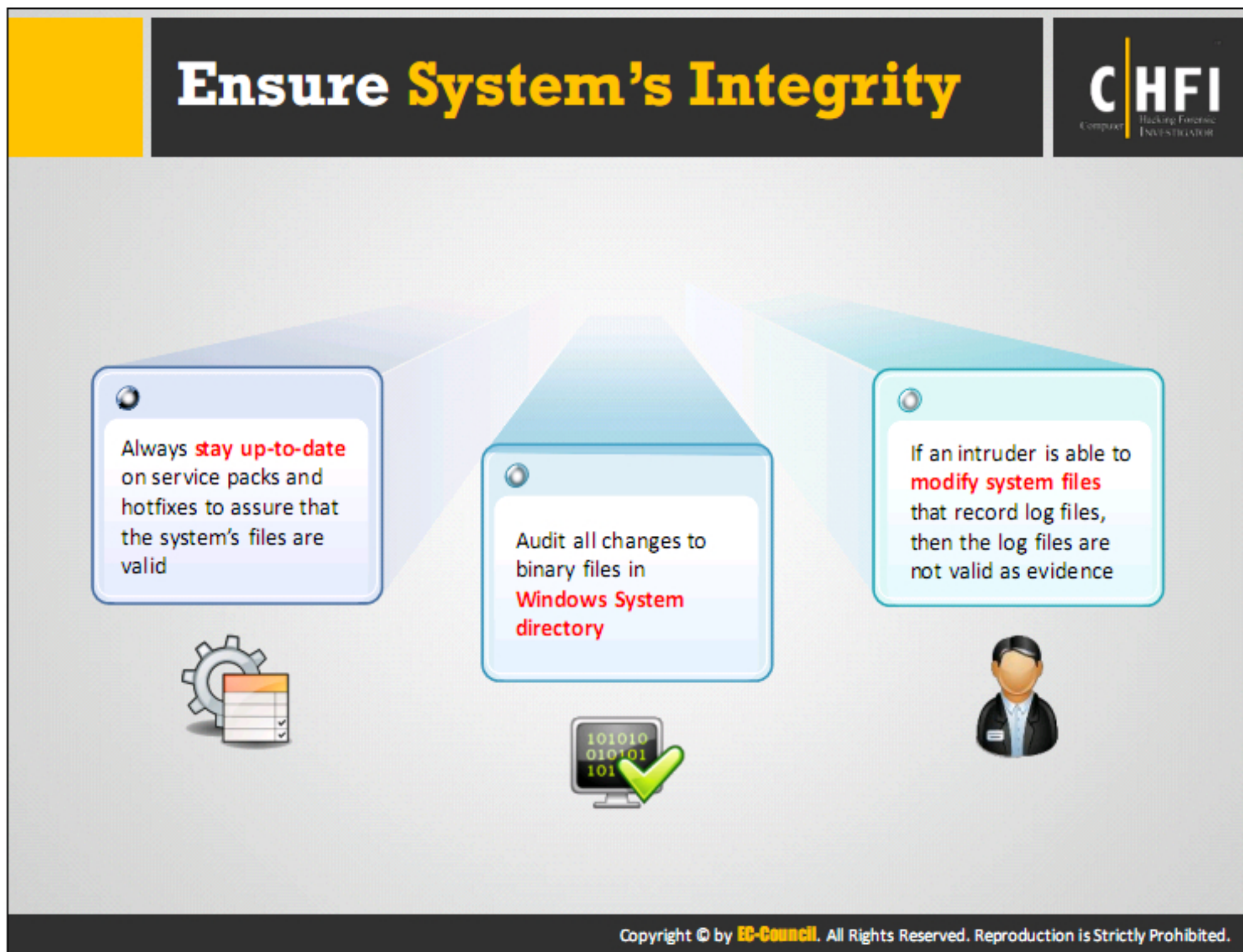
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

IIS centralized binary logging is a process where most of the websites transmit binary and scattered log data to a single log file. Other IIS logging processes generate a separate log file collectively for all websites.

When IIS hosts multiple websites, the process of making many formatted log files and writing the log data to a hard disk consumes CPU and memory resources and thus creates a performance problem. IIS centralized binary logging reduces system resources that are used for logging and provides complete log data for organizations that need it.

It is server property; therefore, all websites present on the server send log data to the central log file. Its log file has an Internet binary log (.ibl) file name extension. This logging is useful when multiple websites are hosted on the same server. By configuring this logging process, the network administrator can monitor network activity and also focus on increasing the number of websites that the server can host. It reduces administration burden for Internet Service Providers (ISPs) and facilitates the gathering and securing of the logged data. For example, if an ISP has four servers with 5,000 websites per server, by configuring IIS centralized binary logging, the ISP can handle 5,000 log files per day per server running IIS.











The system's integrity is the integrity of the data, applications, and software on the system. Ensuring the system's integrity means to preserve and protect the integrity of the entire system. It is very important to maintain the system's integrity because the system holds all the logs pertaining to an intrusion. Failing to fulfill this, the court will not accept the evidence. To achieve the system's integrity, one has to follow the guidelines shown above.



# Control Access to Logs






- 
  - In order to prove the credibility of logs, an investigator or network administrator needs to ensure that any **access to those files is audited**
- 
  - The investigator or administrator can use **NTFS permissions** to secure and audit the log files
- 
  - Web server needs to be **able to write to log files** when the logs are open, but no one else should have access to write to these files
- 
  - Once a log file is closed, no one should have access to modify the **contents of the file**


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Access control is providing privileges to the user, personnel, or an investigator. After the creation of the log file, it is very important to avoid file access or audit by both authorized and unauthorized users. If a log file is properly audited and secured using NTFS permissions, you can have the documented evidence in establishing its credibility. Certain permissions are required to a log file so that the web server can write to the file when the file is open, but once the log file is closed, no resources should have the permission to modify the contents of the file.




# Ensure Log File Authenticity






An investigator can prove that log files are authentic if he or she can prove that the **files have not been altered** since they were originally recorded

**1**



- Log files are generally simple text files that are easy to alter. The date and time stamps on these files are also easy to modify. Hence, they **cannot be considered authentic in their default state.**
- If a server has been compromised, the investigator should **move the logs off the server**

**2**



The logs should be **moved to a master server** and then moved offline to secondary storage media such as a DVD or portable disk

**3**


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


A log file authenticity check is necessary for court proceedings:

- The log files are authentic only if the investigators can prove that they have preserved the integrity of the log files from the time of starting collection.
- Generally, the log files can be easily altered as they are simple text files.
- Even the file date and time stamps are easy to modify. In such a default state, log files can be proved authentic by following a few tips:
  - Move the logs - you must consider that the log files are compromised if a server has been compromised.
  - Move the logs to a master server and then to secondary storage media such as a DVD or disk

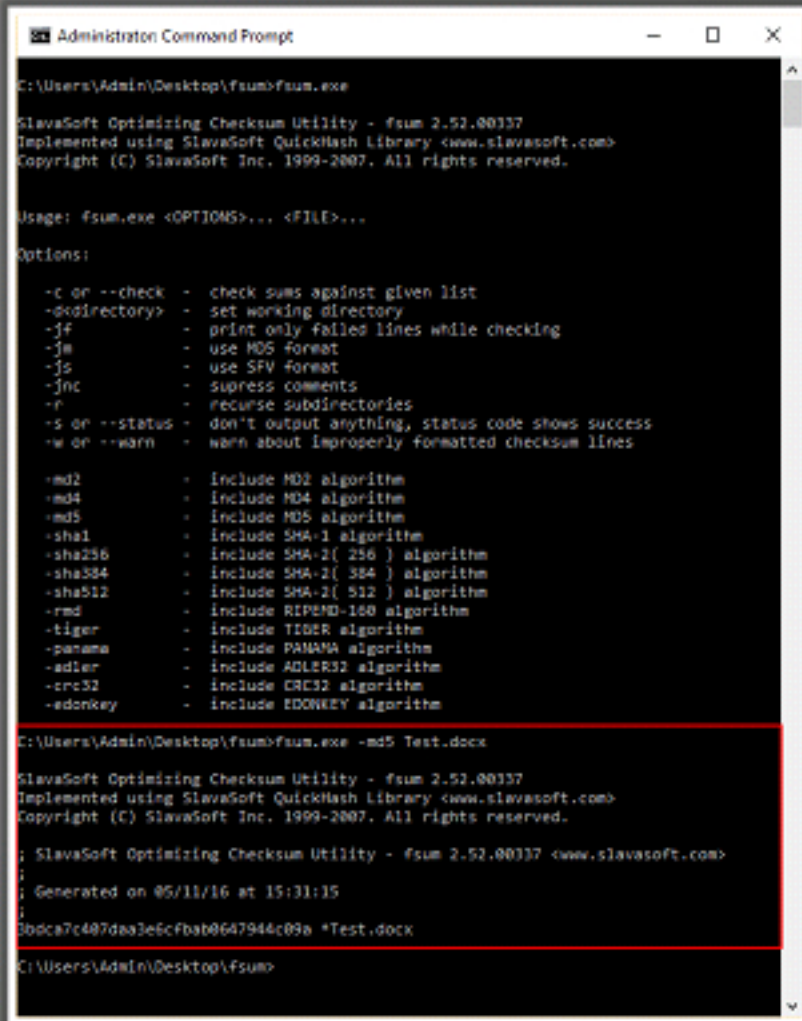


## Use Signatures, Encryption, and Checksums





- The only way to ensure the log file accuracy is to sign and encrypt the log using **PGP** or some other **public-key encryption scheme**
- File signatures are helpful because if a single file is corrupted, it does not invalidate the rest of the logs
- Tools such as **Fsum** can be used to generate **MD5 hashes** for the files
- Store the signatures and hashes with the logs, but also store a secure copy in a separate location



```
Administrator Command Prompt
C:\Users\Admin\Desktop>fsun-fsum.exe

SlavaSoft Optimizing Checksum Utility - fsum 2.52.00337
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2007. All rights reserved.

Usage: fsum.exe <OPTIONS>... <FILE>...

Options:
  -c or --check      - check sums against given list
  -odirectory>      - set working directory
  -ff               - print only failed lines while checking
  -fm              - use MD5 format
  -js              - use SFV format
  -jnc             - suppress comments
  -r               - recurse subdirectories
  -s or --status    - don't output anything, status code shows success
  -w or --warn      - warn about improperly formatted checksum lines

  -md2             - include MD2 algorithm
  -md4             - include MD4 algorithm
  -md5             - include MD5 algorithm
  -sha1            - include SHA-1 algorithm
  -sha256          - include SHA-2( 256 ) algorithm
  -sha384          - include SHA-2( 384 ) algorithm
  -sha512          - include SHA-2( 512 ) algorithm
  -ripemd160       - include RIPEMD-160 algorithm
  -tiger           - include TIGER algorithm
  -panama          - include PANAMA algorithm
  -adler32         - include ADLER32 algorithm
  -crc32           - include CRC32 algorithm
  -edonkey         - include EDONKEY algorithm

C:\Users\Admin\Desktop>fsun-fsum.exe -md5 Test.docx

SlavaSoft Optimizing Checksum Utility - fsum 2.52.00337
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2007. All rights reserved.

; SlavaSoft Optimizing Checksum Utility - fsum 2.52.00337 <www.slavasoft.com>
;
; Generated on 05/11/16 at 15:31:15
;
; 00dca7c407daa3e6cfbab0647944c09a *Test.docx
C:\Users\Admin\Desktop>
```

<http://www.slavasoft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

A signature is the sender's identity sent along with the data. The signature can be integrated with any message, file, or other digitally encoded information, or transmitted separately depending on how a given application functions. A signature is used in public key environments and provides authentication and integrity services.

Encryption is a process of transforming the information using an algorithm to make it unreadable to third-party users, whereas authentic users can decrypt and read the information using the key. To ensure that the log file integrity is maintained, the log is encrypted by using any public-key encryption scheme. Checksum is an error-detection scheme where every message transmitted has a numerical hash value attached, depending on the number of set bits in the message.

Signatures, encryption, and checksums help to prove log authenticity:

- Use a file signature to make the log file more secure
- To generate MD5 hashes for the files, use the Fsum tool
- Store the signature and hashes along with the log
- Store a secure copy in a separate, safe location


### FSUM

Source: <http://www.slavasoft.com>

It is a command line utility for file integrity verification. It offers a choice of 13 hash and checksum functions for file message digest and checksum calculation.



# Work with Copies



- 1** As with all forensic investigations, an investigator should **never work with the original files** when analyzing log files
- 2** The investigator should **create copies** before performing any postprocessing or log file analysis
- 3** If the original files are unaltered, the investigator can prove more **easily** that they are authentic and in their original form
- 4** When using log files as evidence in court, an investigator is required to **present the original files in their original form**

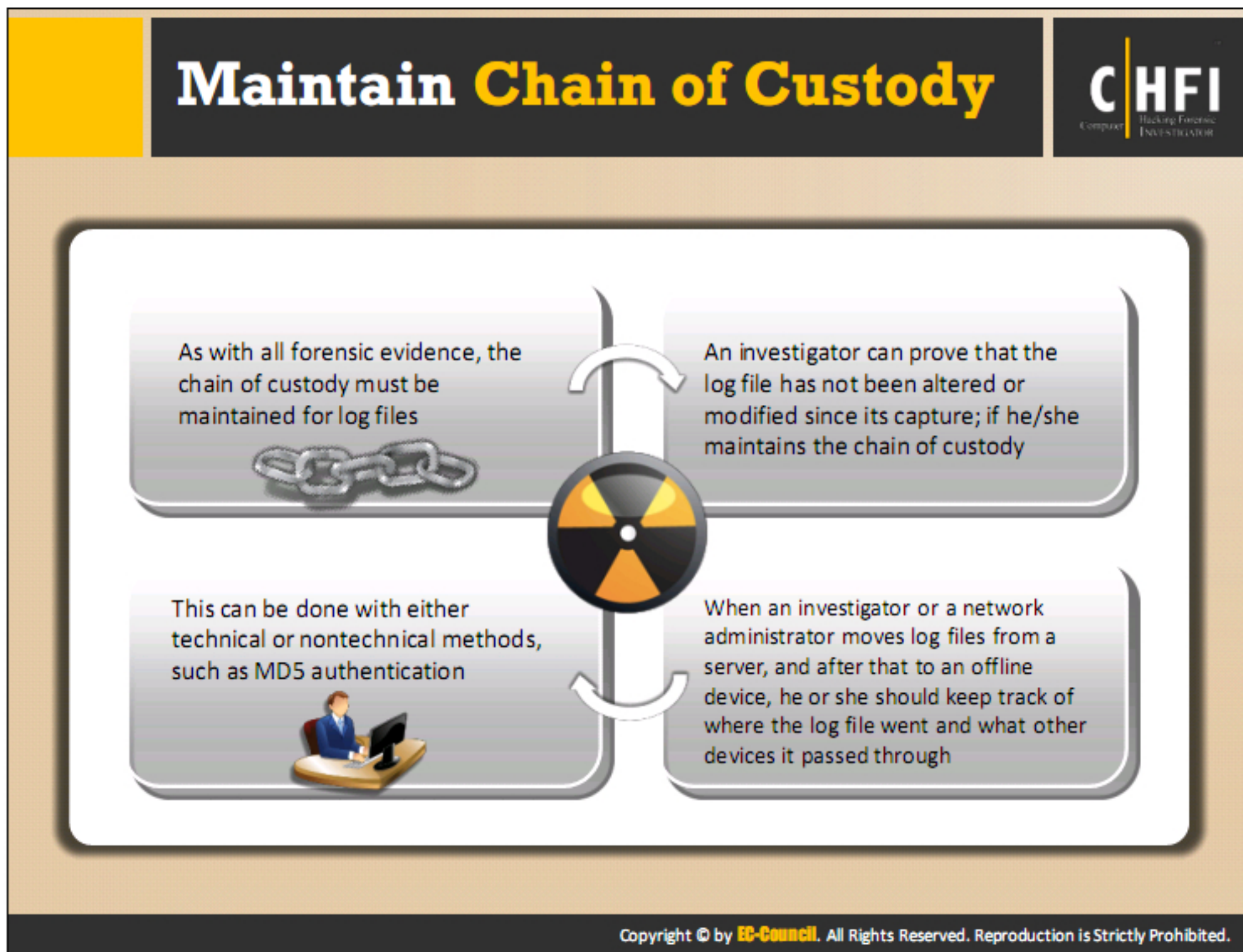
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Original log files are necessary for court proceedings; therefore, it is necessary for an investigator to make copies of the original log files in order to safeguard the originals and produce them in court.

Guidelines for an investigator while performing a log analysis include the following:

- Never perform log file analysis on the original files; make sure to use only copies for this purpose
- It is essential to make copies before performing any log file analysis or post-processing.
- Untouched, original log files are necessary for the investigator or the user to establish the authenticity of the logs in a security incident
- If the investigator uses log files as court evidence, it is necessary to present the original log files in their original form.






Chain of custody is documentation of all the actions taken during an investigation. It not only documents all the actions but also documents information about the evidence and its necessity toward solving the case. When we move the log files from the server and later to an offline device, it is essential to keep track of where the files go. The investigators can use technical or non-technical methods, such as MD5 authentication, to maintain chain of custody.

**MD5 Authentication:** It is an algorithm used to preserve the integrity of the log files. This algorithm uses a 128-bit hash value for the particular log file to protect the file from any kind of alteration.



# Condensing Log File




1

Log files can be sorted by using a **syslog**, but the output of the syslog contains a large log file


2

It is difficult for the forensic team to look for the **important log entry**



3

Log entries need to be **filtered as per the requirement**



4

Tools that can be used:

- **Swatch**  
(<https://sourceforge.net/projects/swatch>)
- **Logcheck** (<http://logcheck.org>)

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Syslogs are the log files that are essential for sorting and routing log messages. With the large number of syslog log files, it becomes difficult for the forensic team to filter the important log entries. For this purpose, it is necessary to use tools such as Swatch and Logcheck for filtering the log files depending on the requirements.

## The tools used are as follows:

### Swatch

Source: <https://sourceforge.net/projects/swatch>

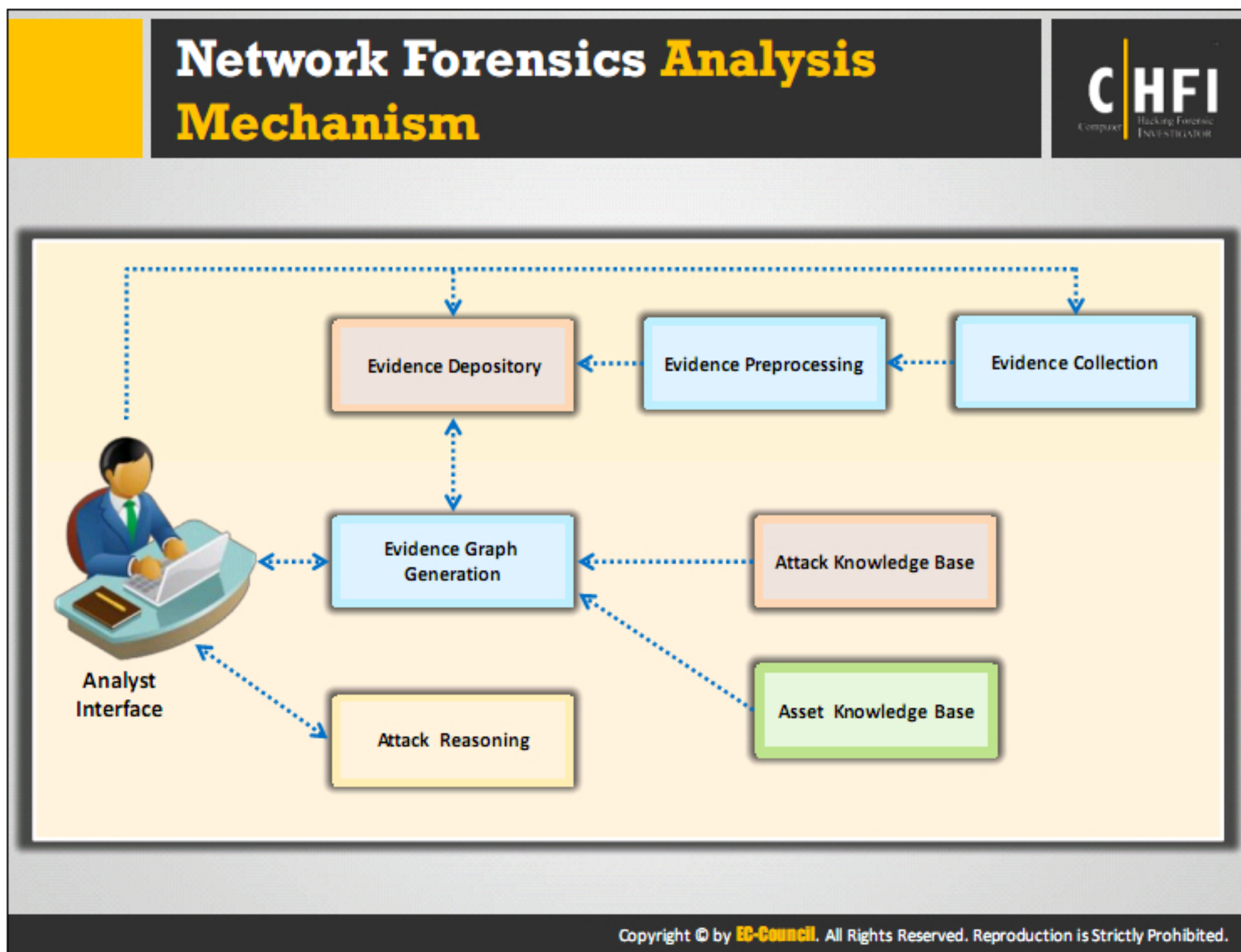
Swatch is a tool used for monitoring log files produced by UNIX's syslog facility

### Logcheck

Source: <http://logcheck.org>

Logcheck is a utility that allows system administrators to view the log files, which are produced by hosts under their control. This is done by mailing summaries of the log files to the hosts, after first filtering out “normal” entries. Normal entries are entries that match one of the many regular expression files contained in the database.





Source: *Building Evidence Graphs for Network Forensic Analysis* - By Wei Wang, Thomas E. Daniels

This network forensics analysis mechanism includes presenting the evidence, manipulating, and automated reasoning.

## Analyst Interface

The analyst interface provides visualization of the evidence graph and reasoning results to the analyst, who passes the feedback to the graph generation and reasoning components.

## Evidence Collection

Evidence collection involves the collection of intrusion evidence from networks and hosts under investigation.

## Evidence Preprocessing

Evidence preprocessing deals with the analysis of assertive types of evidence, such as intrusion alerts, into the appropriate format and reduces the repetition in low-level evidence by aggregation.

## Evidence Depository

After preprocessing, the collected intrusion evidence is stored in the evidence depository.



## **Evidence Graph Generation**

Evidence graph manipulation generates and updates the evidence graph using intrusion evidence from the depository.

## **Attack Reasoning**

Attack reasoning is the process of automated reasoning based on the evidence graph.

## **Attack Knowledge Base**

The attack knowledge base includes knowledge of prior exploits.

## **Asset Knowledge Base**

The asset knowledge base includes knowledge of the networks from the fundamentals and hosts under investigation.

In the initial phase, the evidence collected is pre-processed and stored in the evidence depository. The graph generation module builds the evidence graph with the evidence retrieved from the depository. Next, the reasoning module derives the automated inference based on the evidence graph and presents the results to the analyst. Through the interface module, the analyst can provide expert opinions and out-of-band information, mainly via two approaches:

1. Edit the evidence graph directly.
2. Send queries to retrieve specific evidence.

Next, the reasoning process is performed on the updated evidence graph for better results.

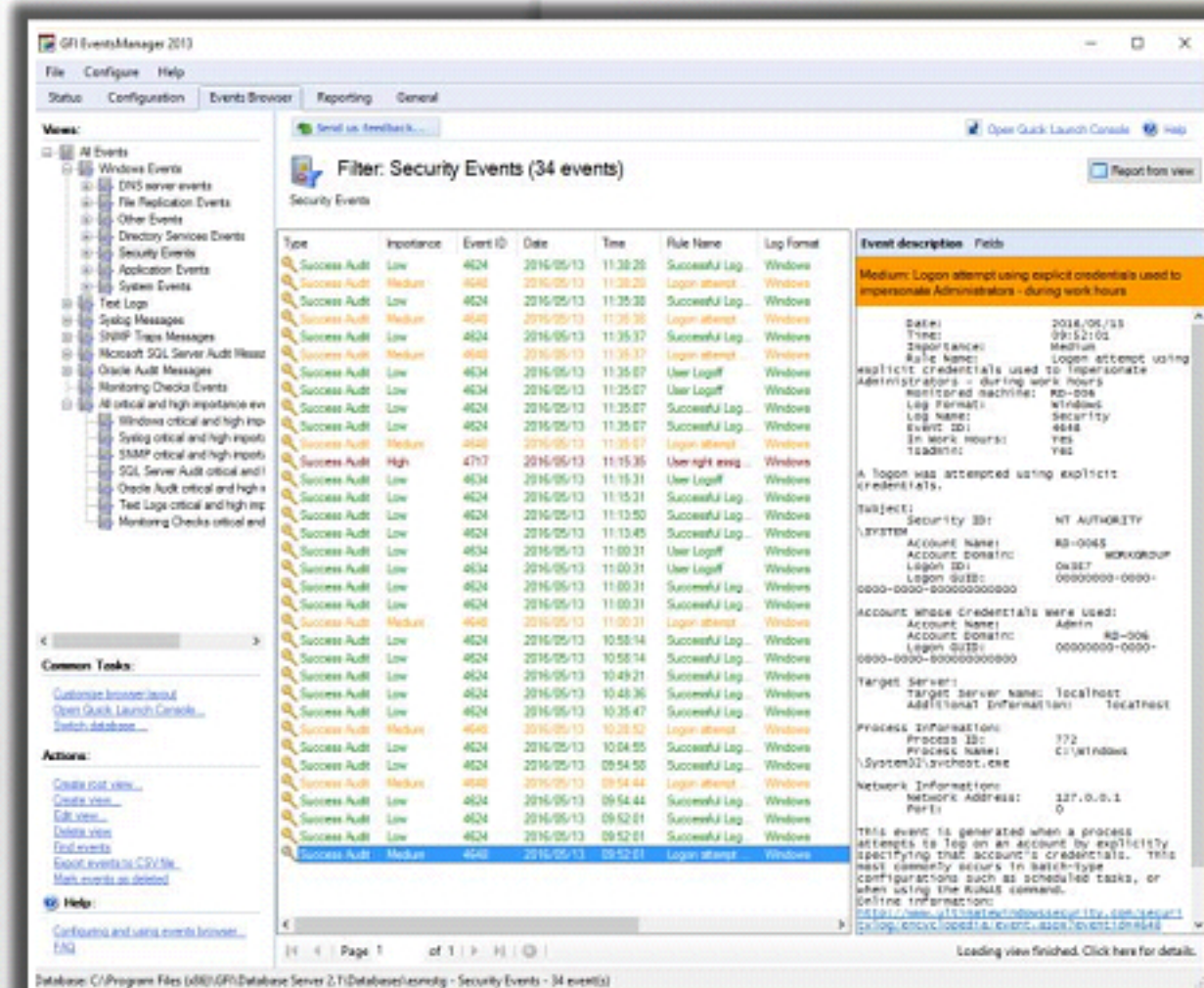


# Log Capturing and Analysis

## Tools: GFI EventsManager



- GFI EventsManager enables to **manage event log data** for system reliability, security, availability, and compliance
- It enables **increased uptime** by collecting, normalizing, analyzing, categorizing and consolidating log data from multiple sources across the network



<http://www.gfi.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

### Features:

- Analysis of log data, including SNMP traps, Windows® event logs, W3C logs, text-based logs, Syslog, SQL Server®, and Oracle® audit logs
- Provides specific reports for some of the major compliance acts as well as other standard reports
- Filter-enabled charts provide access to the important data you need
- GFI EventsManager offers deep granular control of log data to easily classify the information from the system.
- GFI EventsManager offers safe storage of log data according to industry standards and security best practices.

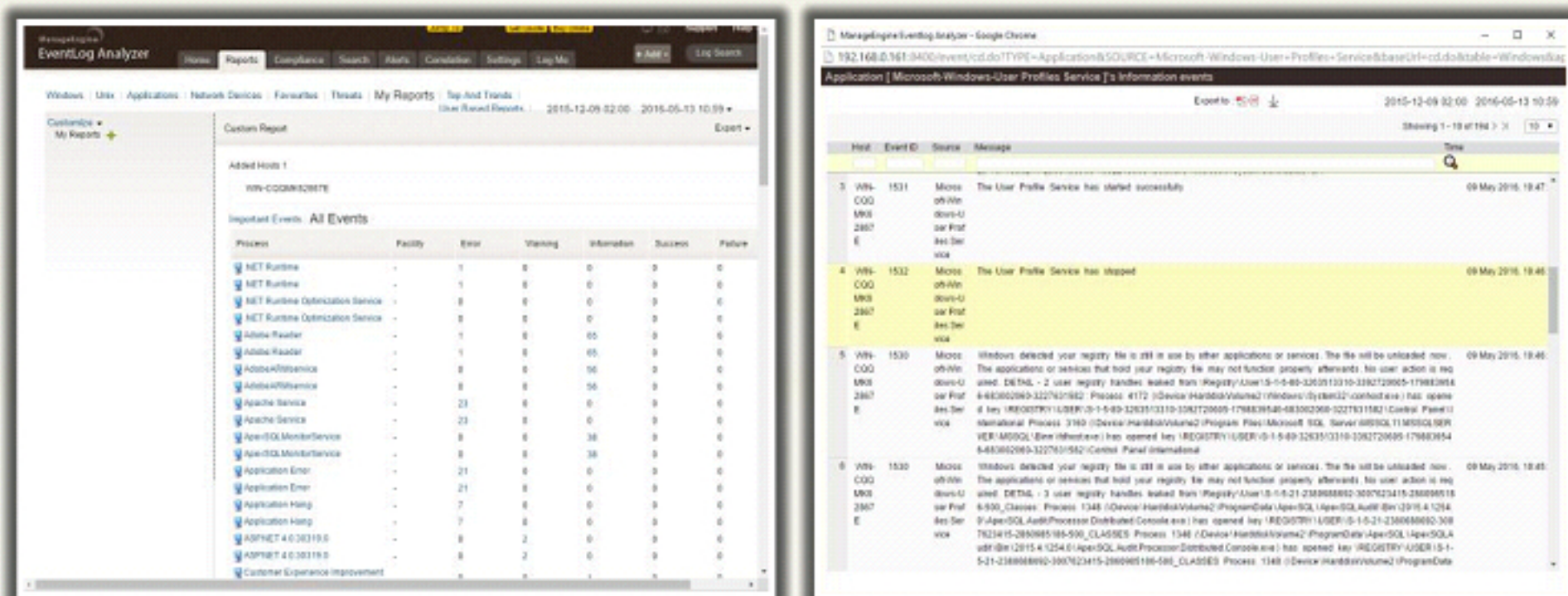


# Log Capturing and Analysis

## Tools: EventLog Analyzer



- EventLog Analyzer allows organizations to **automate the process of managing machine generated logs** by collecting, analyzing, correlating, searching, reporting, and archiving from one central location



<https://www.manageengine.com>


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.











### Features:

- Offers log management for network security
- Monitors application Logs and generates reports
- Stays informed on event activities in real-time
- Offers holistic approach for network IT security
- Checks if audit is ready and compliant



## Log Capturing and Analysis Tools (Cont'd)



 <b>Kibana</b> <a href="https://www.elastic.co">https://www.elastic.co</a>	 <b>OSSEC</b> <a href="http://ossec.github.io">http://ossec.github.io</a>
 <b>Syslog-ng</b> <a href="https://syslog-ng.org">https://syslog-ng.org</a>	 <b>Ipswitch Log Management</b> <a href="https://www.ipswitch.com">https://www.ipswitch.com</a>
 <b>RSYSLOG</b> <a href="http://www.rsyslog.com">http://www.rsyslog.com</a>	 <b>Veriato Server Manager</b> <a href="http://www.veriato.com">http://www.veriato.com</a>
 <b>Firewall Analyzer</b> <a href="https://www.manageengine.com">https://www.manageengine.com</a>	 <b>Log Management Utility</b> <a href="http://www.biz.konicaminolta.com">http://www.biz.konicaminolta.com</a>
 <b>Simple Event Correlator (SEC)</b> <a href="https://simple-evcorr.github.io">https://simple-evcorr.github.io</a>	 <b>Snare</b> <a href="https://www.intersectalliance.com">https://www.intersectalliance.com</a>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Kibana

Source: <https://www.elastic.com>

Kibana is an open-source data visualization platform that allows interaction with the data through a graphical user interface.

## Syslog-ng

Source: <https://syslog-ng.org>

syslog-ng allows the collection, parsing, classification, and correlation of logs from across the infrastructure and store or route them to log analysis tools.

## RSYSLOG

Source: <http://www.rsyslog.com>

RSYSLOG is a system for log processing. It offers security features and a modular design. It accepts inputs from a variety of sources, transforms them, and outputs the results to diverse destinations.

## Firewall Analyzer

Source: <https://www.manageengine.com>

ManageEngine Firewall Analyzer is a log analytics and configuration management software that helps network administrators to collect, archive, analyze their security device logs and subsequently generate forensic reports.



## Simple Event Correlator (SEC)

Source: <https://simple-evcorr.github.io>

SEC is an event correlation tool for event processing, which can be harnessed for event log monitoring, network and security management, fraud detection, and any other task that involves event correlation.

## OSSEC

Source: <http://ossec.github.io>

OSSEC is an open-source host-based intrusion detection system. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting, and active response. It runs on operating systems such as Linux, OpenBSD, FreeBSD, Mac OS X, Solaris, and Windows.

## Ipswitch Log Management

Source: <https://www.ipswitch.com>

The Ipswitch Log Management Suite is an automated tool that collects, stores, archives, and backs-up Syslog, Windows events, or W3C/IIS logs. It analyzes for suspicious activities and automatically generates compliance reports.

## Veriato Server Manager

Source: <http://www.veriato.com>

This tool allows the viewing and reporting of event log data and isolates pertinent log entries by merging multiple logs into a single view, hiding duplicate entries, and filtering the results. It easily exports, prints, or emails the results for clear and concise event log analysis.

## Log Management Utility

Source: <http://www.biz.konicaminolta.com>

Log Management Utility enables one to collect, save, browse, and search MFP Audit Logs smoothly and for a longer period of time from a PC, giving more time to manage and analyze the conditions of each MFP.


## Snare











Source: <https://www.intersectalliance.com>

Snare helps in gathering and filtering IT-event data for critical security monitoring, analysis, auditing, and archiving.



## Log Capturing and Analysis Tools (Cont'd)



 <b>Splunk Enterprise</b> <a href="http://www.splunk.com">http://www.splunk.com</a>	 <b>Logscale</b> <a href="http://logscale.com">http://logscale.com</a>
 <b>Loggly</b> <a href="https://www.loggly.com">https://www.loggly.com</a>	 <b>ArcSight ESM</b> <a href="http://www8.hp.com">http://www8.hp.com</a>
 <b>vRealize Log Insight</b> <a href="http://www.vmware.com">http://www.vmware.com</a>	 <b>Xpolog Log Management</b> <a href="http://www.xpolog.com">http://www.xpolog.com</a>
 <b>Sumo Logic</b> <a href="https://www.sumologic.com">https://www.sumologic.com</a>	 <b>LogRhythm</b> <a href="https://www.logrhythm.com">https://www.logrhythm.com</a>
 <b>TIBCO LogLogic</b> <a href="http://www.tibco.com">http://www.tibco.com</a>	 <b>Sawmill</b> <a href="https://www.sawmill.net">https://www.sawmill.net</a>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Splunk Enterprise

Source: <http://www.splunk.com>

Splunk Enterprise allows investigators to collect, analyze, and act upon the untapped value of the big data generated by the technology infrastructure, security systems, and business applications—giving them insights to drive operational performance and business results.

## Loggly

Source: <https://www.loggly.com>

Loggly offers a cloud-based service that mines log data in real time and reveals what is required, so that you have the insights you need to produce.

## vRealize Log Insight

Source: <http://www.vmware.com>

vRealize Log Insight delivers heterogeneous and scalable log management with intuitive, actionable dashboards, sophisticated analytics, and broad third-party extensibility, thereby providing operational visibility and faster troubleshooting.

## Sumo Logic

Source: <https://www.sumologic.com>

Sumo Logic is used to build, run, and secure modern applications. It is a cloud-native, machine data analytics service for log management and time series metrics.



## **TIBCO LogLogic**

Source: <http://www.tibco.com>

This tool is used to harness log and machine data to provide insight into IT operational efficiencies.

## **Logscape**

Source: <http://logscape.com>

This tool allows searching, visualizing, and analyzing log files and operational data.

## **ArcSight ESM**

Source: <http://www8.hp.com>

HPE Security ArcSight ESM is a security management application that combines event correlation and security analytics to identify and prioritize threats in real time, thereby facilitating immediate response and remediation.

## **XpoLog Log Management**

Source: <http://www.xpolog.com>

The XpoLog log management platform helps in the analysis, visualization, monitoring, and automated in-depth mining of log data. XpoLog allows the optimization of IT operations and visibility for any type of system log data.

## **LogRhythm**

Source: <https://www.logrhythm.com>

The LogRhythm security intelligence and analytics platform enables organizations to detect, prioritize, and neutralize cyber threats that penetrate the perimeter or originate from within.


## **Sawmill**











Source: <https://www.sawmill.net>

Sawmills helps analyze, monitor, and alert a wide range of systems. It provides log processing and reporting features to gain insight into the network data.



## Log Capturing and Analysis Tools (Cont'd)



 <b>McAfee Enterprise Log Manager</b> <a href="http://www.mcafee.com">http://www.mcafee.com</a>	 <b>Event Log Explorer</b> <a href="http://www.eventlogxp.com">http://www.eventlogxp.com</a>
 <b>Log &amp; Event Manager</b> <a href="http://www.solarwinds.com">http://www.solarwinds.com</a>	 <b>WebLog Expert</b> <a href="https://www.weblogexpert.com">https://www.weblogexpert.com</a>
 <b>Papertrail</b> <a href="https://papertrailapp.com">https://papertrailapp.com</a>	 <b>ELM Enterprise Manager</b> <a href="http://tntsoftware.com">http://tntsoftware.com</a>
 <b>EventReporter</b> <a href="http://www.eventreporter.com">http://www.eventreporter.com</a>	 <b>EventSentry</b> <a href="http://www.eventsentry.com">http://www.eventsentry.com</a>
 <b>Kiwi Log Viewer</b> <a href="http://www.kiwisyslog.com">http://www.kiwisyslog.com</a>	 <b>LogMeister</b> <a href="http://www.logmeister.com">http://www.logmeister.com</a>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### McAfee Enterprise Log Manager

Source: <http://www.mcafee.com>

McAfee Enterprise Log Manager collects, compresses, signs, and stores all original events with a clear audit trail of activity that cannot be repudiated.

### Log and Event Manager

Source: <http://www.solarwinds.com>

Log & Event Manager is an SIEM that makes it easy to use logs for security, compliance, and troubleshooting.

### Papertrail

Source: <https://papertrailapp.com>

Papertrail is used for its time-saving log tools, flexible system groups, team-wide access, long-term archives, charts, analytics exports, and monitoring webhooks.

### EventReporter

Source: <http://www.eventreporter.com>

EventReporter is a Windows event log processor and syslog forwarder. It is used to consolidate multiple event logs and create a central repository.



## **Kiwi Log Viewer**

Source: <http://www.kiwisyslog.com>

Kiwi Log Viewer enables the monitoring of a log file for changes. It can display changes in real-time and allows automatic monitoring of log file entries for specific keywords, phrases, or patterns.

## **Event Log Explorer**

Source: <http://www.eventlogxp.com>

Event Log Explorer is a software solution for viewing, analyzing and monitoring events recorded in Microsoft Windows event logs. Event Log Explorer simplifies the analysis of event logs (security, application, system, setup, directory service, DNS, and others).

## **WebLog Expert**

Source: <https://www.weblogexpert.com>

WebLog Expert is an access log analyzer. It provides information about a website's visitors: activity statistics, accessed files, paths through the site, information about referring pages, search engines, browsers, operating systems, and more. WebLog Expert can analyze logs of Apache, IIS and Nginx web servers. It can even read GZ and ZIP compressed log files, which precludes the need for manually unpacking them.

## **ELM Enterprise Manager**

Source: <http://tntsoftware.com>

ELM Enterprise Manager elevates Windows event log monitoring to real-time. Events logs are collected reliably after they are written.

## **EventSentry**

Source: <http://www.eventsentry.com>

It receives critical alerts and consolidates all your logs in one place with real-time event log, log file, and Syslog monitoring. It offers sophisticated rule sets to ensure you only get the alerts you need. It also offers web-based reporting which gives you a unique insight into all of your logs.


## **LogMeister**











Source: <http://www.logmeister.com>

This tool monitors Windows event logs, syslog, and text logs on servers throughout a network, providing notifications of key events and allowing for appropriate and timely action. It consolidates, archives, transforms, and exports the log data to meet the required compliance needs.



## Log Capturing and Analysis Tools (Cont'd)



 <b>InTrust</b> <a href="http://software.dell.com">http://software.dell.com</a>	 <b>MyEventViewer</b> <a href="http://www.nirsoft.net">http://www.nirsoft.net</a>
 <b>Alert Logic Log Manager</b> <a href="https://www.alertlogic.com">https://www.alertlogic.com</a>	 <b>WinAgents EventLog Translation Service</b> <a href="http://www.winagents.com">http://www.winagents.com</a>
 <b>Sentinel Log Manager</b> <a href="https://www.netiq.com">https://www.netiq.com</a>	 <b>EventTracker Enterprise</b> <a href="http://www.eventtracker.com">http://www.eventtracker.com</a>
 <b>Tripwire Log Center</b> <a href="http://www.tripwire.com">http://www.tripwire.com</a>	 <b>Logstash</b> <a href="http://www.netwrix.com">http://www.netwrix.com</a>
 <b>AlienVault Unified Security Management</b> <a href="https://www.alienvault.com">https://www.alienvault.com</a>	 <b>SecurityCenter CV</b> <a href="https://www.tenable.com">https://www.tenable.com</a>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### InTrust

Source: <http://software.dell.com>

InTrust enables the secure collection, storage, search, and analysis of massive amounts of IT data from numerous data sources, systems, and devices in one place.

### Alert Logic Log Manager

Source: <https://www.alertlogic.com>

Alert Logic Log Manager with ActiveWatch is a Security-as-a-Service (SaaS) solution that meets compliance requirements and identifies security issues across the entire environment, including public cloud. It collects, processes, and analyzes data.

### Sentinel Log Manager

Source: <https://www.netiq.com>

Sentinel™ Log Manager is a software appliance that enables the collection, storage, analysis, and management of IT infrastructure event and security logs.

### Tripwire Log Center

Source: <http://www.tripwire.com>

Tripwire Log Center normalizes data from servers, security and network devices, as well as applications, integrating them with Tripwire Enterprise and Tripwire IP360™ to provide



endpoint protection and security. Tripwire Log Center ensures that regulations are met with complete, secure, and reliable log collection.

### **AlienVault Unified Security Management**

Source: <https://www.alienvault.com>

AlienVault Unified Security Management™ (USM) is a platform that provides unified, coordinated security monitoring, security event management and reporting, continuous threat intelligence and multiple security functions without multiple consoles.

### **MyEventViewer**

Source: <http://www.nirsoft.net>

MyEventViewer allows the users to watch multiple event logs in one list. Additionally, MyEventViewer allows easy selection of multiple event items and saving them to HTML/Text/XML file or copying them to the clipboard (Ctrl+C) and pasting them into Excel.

### **WinAgents EventLog Translation Service**

Source: <http://www.winagents.com>

The WinAgents EventLog Translation Service is a server that monitors Windows event logs and forwards the events that appear for further processing. The program can forward events to a Syslog server or to an SNMP management station.

### **EventTracker Enterprise**

Source: <http://www.eventtracker.com>

EventTracker Enterprise is a log management tool and includes features such as File Integrity Monitoring, Change Audit, Config Assessment, Cloud Integration, Event Correlation, and writeable media monitoring.

### **Logstash**

Source: <http://www.netwrix.com>

Logstash is a data pipeline that helps the processing of logs and other event data from a variety of systems. Logstash can connect to a variety of sources and stream data at scale to a central analytics system. It provides a convenient way to custom logic for parsing these logs at scale.


### **SecurityCenter CV**











Source: <https://www.tenable.com>

SecurityCenter Continuous View (SecurityCenter CV) collects data from multiple sensors to provide advanced analysis of vulnerability, threat, network traffic, and event information and delivers a continuous view of IT security across the environment.



## Log Capturing and Analysis Tools (Cont'd)



 <b>The Elastic Stack</b> <a href="https://www.elastic.co">https://www.elastic.co</a>	 <b>Logsene</b> <a href="https://www.sematext.com">https://www.sematext.com</a>
 <b>CorreLog</b> <a href="https://correlog.com">https://correlog.com</a>	 <b>SaaS Log Management</b> <a href="http://www.cloudaccess.com">http://www.cloudaccess.com</a>
 <b>Assuria Log Manager</b> <a href="http://www.assuria.com">http://www.assuria.com</a>	 <b>ApexSQL Log</b> <a href="http://www.apexsql.com">http://www.apexsql.com</a>
 <b>BlackStratus LOGStorm</b> <a href="http://www.blackstratus.com">http://www.blackstratus.com</a>	 <b>FortiSIEM</b> <a href="https://www.fortinet.com">https://www.fortinet.com</a>
 <b>PowerBroker Event Vault</b> <a href="https://www.beyondtrust.com">https://www.beyondtrust.com</a>	 <b>Graylog</b> <a href="https://www.graylog.org">https://www.graylog.org</a>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

### The Elastic Stack

Source: <https://www.elastic.co>

The open-source Elastic Stack, that is Elasticsearch, Kibana, Logstash, and Beats, helps procure data from any source in any format and search, analyze, and visualize it in real time.

### CorreLog

Source: <https://correlog.com>

CorreLog is a solution for cross-platform IT security log management and event log correlation. It allows real-time event log collection across both distributed and mainframe systems. Event logs generated from CorreLog Agents are ready-format for the CorreLog SIEM Correlation Server or any SIEM correlation engine.

### Assuria Log Manager

Source: <http://www.assuria.com>

This tool is used for the collection of forensically sound logs from almost any source into a central store. It allows enterprise-wide automated management of logs, including log rotation.



## **BlackStratus LOGStorm**

Source: <http://www.blackstratus.com>

LOGStorm™ is a log management and log monitoring solution that combines log management with correlation technology, real-time event log correlation and log monitoring, and an integrated incident response system.

## **PowerBroker Event Vault**

Source: <https://www.beyondtrust.com>

BeyondTrust PowerBroker Event Vault automates and streamlines the collection and management of standard Microsoft Windows event logs.

## **Logsene**

Source: <https://www.sematext.com>

Using Logsene, all logs are accessible in one place. It allows to inspect logs via UI or Elasticsearch API and correlate logs with performance metrics via SPM

## **SaaS Log Management**

Source: <http://www.cloudaccess.com>

SaaS Log Management is a solution that works with CloudAccess SIEM Log management to provide secure storage and full lifecycle management of event data.

## **ApexSQL Log**

Source: <http://www.apexsql.com>

ApexSQL Log is a SQL Server database transaction log reader that can present all the information in a human readable format.

## **FortiSIEM**

Source: <https://www.fortinet.com>

It is a Security Information and Event Management (SIEM) used for the detection and remediation of security events. It offers security, performance, and compliance management.


## **Graylog**

Source: <https://www.graylog.org>

It is an open-source log management tool used to search, analyze, and generate alerts across all log files.



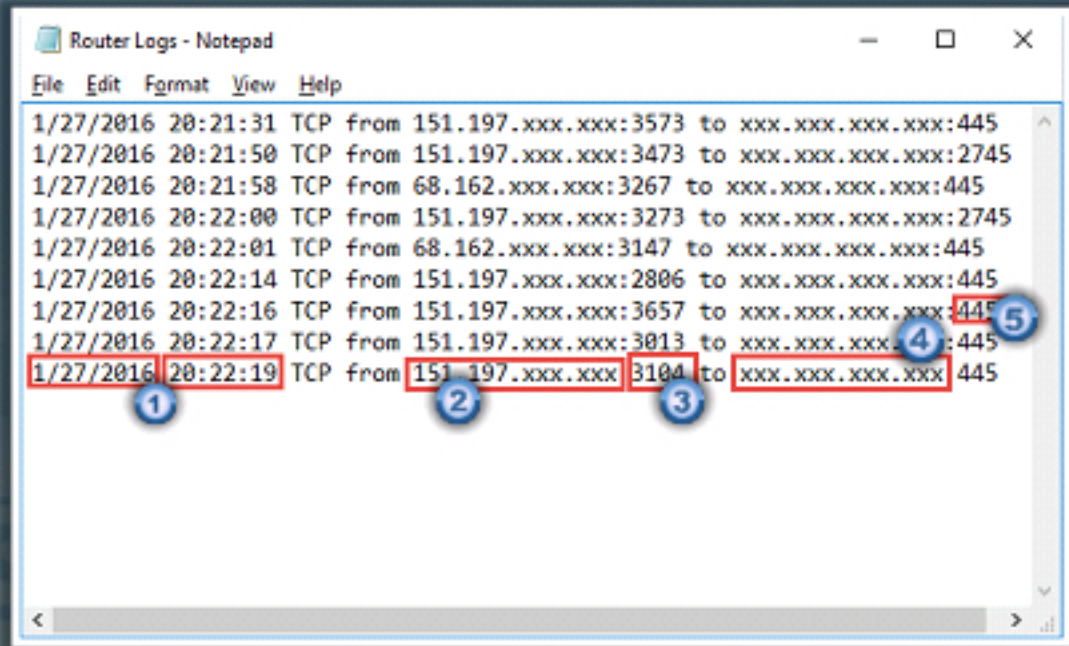
# Analyzing Router Logs



- ❑ Routers **store network connectivity logs** with details such as date, time, source and destination IPs and Ports used
- ❑ This information can **help investigators in verifying the timestamps of an attack** and correlate various events to find the source and destination IP
- ❑ Routers **have many standards for storing the log** details of a network

The incoming log details are as follows:

1. Date and time
2. Source IP address
3. Source-port
4. Destination IP address
5. Destination-port



```
Router Logs - Notepad
File Edit Format View Help
1/27/2016 20:21:31 TCP from 151.197.xxx.xxx:3573 to xxx.xxx.xxx.xxx:445
1/27/2016 20:21:50 TCP from 151.197.xxx.xxx:3473 to xxx.xxx.xxx.xxx:2745
1/27/2016 20:21:58 TCP from 68.162.xxx.xxx:3267 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:00 TCP from 151.197.xxx.xxx:3273 to xxx.xxx.xxx.xxx:2745
1/27/2016 20:22:01 TCP from 68.162.xxx.xxx:3147 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:14 TCP from 151.197.xxx.xxx:2806 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:16 TCP from 151.197.xxx.xxx:3657 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:17 TCP from 151.197.xxx.xxx:3013 to xxx.xxx.xxx.xxx:445
1/27/2016 20:22:19 TCP from 151.197.xxx.xxx:3104 to xxx.xxx.xxx.xxx:445
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In a network forensic investigation, the investigator collects the logs of a router to examine and determine the details such as IP addresses and the protocols. Redirection of the logs to syslog server is done in the following manner:

```
#config terminal Logging 192.168.1.1
```

During any network hacking, or unauthorized access scenarios, all the logs pertaining to the attack will be stored in the compromised device, which may be the router/switch, database, IDS, the ISP router, or application server. Almost all the professional network devices allow logging of the events; however, due to memory constraints, these devices cannot store the logs for long durations. Therefore, the administrators collect and store these logs on a regular basis.

From the collected logs, one has to identify, collect, and save the suspicious logs along with the firewall protocols for investigation purposes. Log analysis can be completed either manually or with the help of log-analyzing tools. After analyzing the logs, filters are applied to eliminate unnecessary data.



## Evidence Gathering from ARP Table



The ARP table of a router comes in handy for investigating network attacks, as the table **contains IP addresses associated with the respective MAC addresses**



An investigator can view the ARP table in Windows by issuing the command **arp -a**



The ARP table maintained on the router is of crucial importance, as it can provide information about the MAC address of all the hosts that were involved in recent communications

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>arp -a


Interface: 10.10.10.2 --- 0xc
Internet Address      Physical Address      Type
10.10.10.1             00-15-5d-c7-22-d4     dynamic
10.10.10.255           ff-ff-ff-ff-ff-ff     static
224.0.0.22             01-00-5e-00-00-16     static
224.0.0.252            01-00-5e-00-00-fc     static

C:\Windows\system32>
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

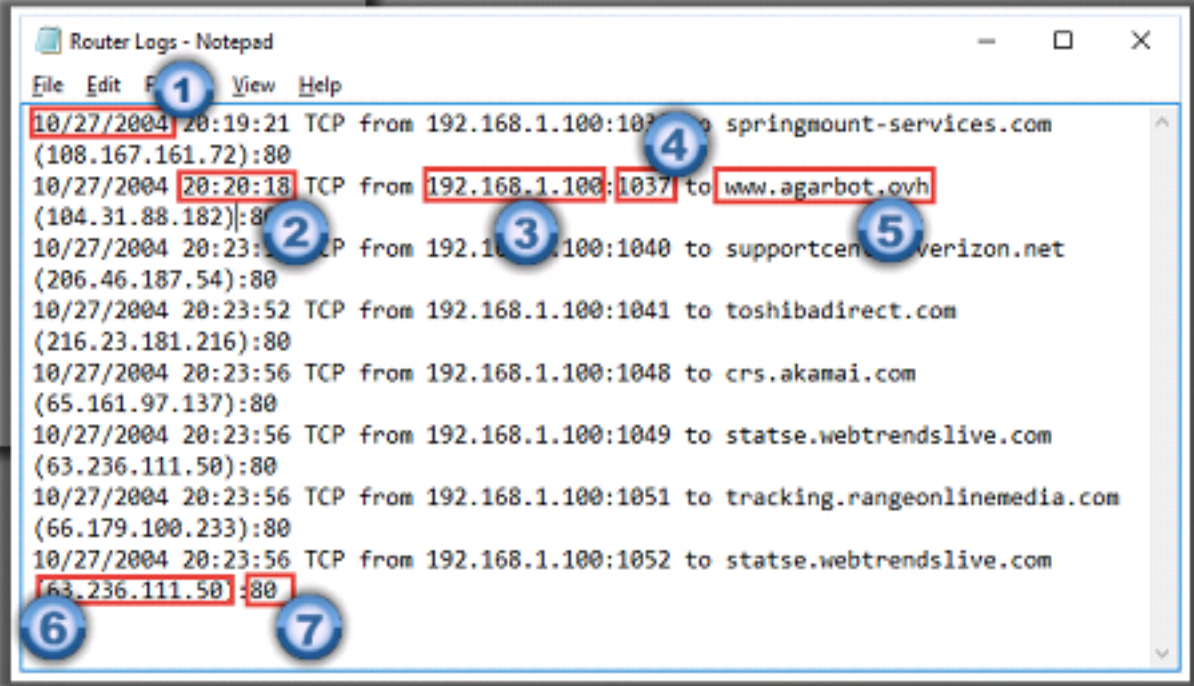


## Analyzing Router Logs (Cont'd)



The outgoing log details are as follows:

1. Date
2. Time
3. Source IP address
4. Source-port
5. URL accessed
6. URL IP address
7. Port Used



```
Router Logs - Notepad
File Edit View Help
10/27/2004 20:19:21 TCP from 192.168.1.100:1037 to springmount-services.com
(108.167.161.72):80
10/27/2004 20:20:18 TCP from 192.168.1.100:1037 to www.agarbot.ovh
(104.31.88.182):80
10/27/2004 20:23:56 TCP from 192.168.1.100:1040 to supportcenter.verizon.net
(206.46.187.54):80
10/27/2004 20:23:52 TCP from 192.168.1.100:1041 to toshibadirect.com
(216.23.181.216):80
10/27/2004 20:23:56 TCP from 192.168.1.100:1048 to crs.akamai.com
(65.161.97.137):80
10/27/2004 20:23:56 TCP from 192.168.1.100:1049 to statse.webtrendsllive.com
(63.236.111.50):80
10/27/2004 20:23:56 TCP from 192.168.1.100:1051 to tracking.rangeonlinemedia.com
(66.179.100.233):80
10/27/2004 20:23:56 TCP from 192.168.1.100:1052 to statse.webtrendsllive.com
(63.236.111.50):80
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Routers follow different standards for storing a log in a network. It is not necessary that every router follows the same standard. For example, in the above screenshot, the log file contains details such as date, time, source IP address, source-port, URL accessed, URL's IP address, and port used. These details might be helpful for the investigators during the investigations. The syntax of a log file from another router may differ.



## Analyzing Router Logs: Cisco



- Cisco routers run on specific operating system, the **Cisco IOS**
- The OS has a built in security manager that **defines policies regarding basic logging parameters**
- The router **complies with syslog standards** to define severity levels using numeric code

Level	System	Description
Emergency	0	System unusable messages
Alert	1	Immediate action required messages
Critical	2	Critical condition messages
Error	3	Error condition messages
Warning	4	Warning condition messages
Notification	5	Normal but significant messages
Information	6	Informational messages
Debugging	7	Debugging messages

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Cisco Networking Software IOS is the networking software used in Cisco routers. The IOS integrates business-critical services and hardware platform support. The IOS security technologies act as a shield for the business process against attack and disruption and protect privacy, as well as support policy and regulatory compliance controls.

Transit network devices contain syslog messages that provide insight and brief a context of a security instance. This insight aids in determining the validity and extent of an incident. Within the context of a security incident, administrators can use syslog messages to understand communication relationships; timing; and, in some cases, the attacker's motives and/or tools. The events come into consideration as complementary and are required to be used in conjunction with other forms of network monitoring that may already be in place.

There are eight severity levels of classification of the syslog messages on Cisco IOS routers. There is a number and a corresponding name for each severity level for identification. The lower the number is, the greater is the severity of the message, as shown in the following table.

Source: <http://www.cisco.com>



## Analyzing Router Logs: Cisco (Cont'd)



Cisco IOS helps users to classify logs using certain predefined identifiers such as:

Mnemonic	Severity	Description
%SEC-6-IPACCESSLOGDP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGNP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGP	6	A packet matching the log criteria for the given access list has been detected (TCP or UDP)
%SEC-6-IPACCESSLOGRL	6	Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available.
%SEC-6-IPACCESSLOGRP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGS	6	A packet matching the log criteria for the given access list was detected.
%SEC-4-TOOMANY	4	The system was not able to process the packet because there was not enough room for all of the desired IP header options. The packet has been discarded.
%IPV6-6-ACCESSLOGP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGDP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGNP	6	A packet matching the log criteria for the given access list was detected.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cisco ASA provides log messages that are useful in CISCO IOS software. Router log messages do not contain numerical identifiers that assist in identifying the messages. Mentioned below is a list of router log messages with detailed description, which are most likely to be useful when analyzing security-related incidents. However, many organizations do not make extensive use of logging on routers and because router logging is somewhat limited, and NetFlow is often a more effective means of analysis.

Source: <http://www.cisco.com>



## Analyzing Router Logs: Cisco (Cont'd)



■ The Cisco router log details are as follows:

- |               |                           |
|---------------|---------------------------|
| 1. Event ID   | 5. Protocol applied       |
| 2. Date       | 6. Source IP address      |
| 3. Time       | 7. Destination IP address |
| 4. Identifier |                           |



```
002416 Feb 22 2016 11:51:07.149 EDT: %SEC-6-IPACCESSLOGP: list 185 denied  
tcp 172.16.1.14(95) -> 192.168.2.1(418), 1 packet [0x279C8521]  
002417: Feb 22 2016 11:51:09.153 EDT: %SEC-6-IPACCESSLOGP: list 185 denied  
tcp 172.16.1.14(7331) -> 192.168.2.1(428), 1 packet [0x279C8521]  
002418: Feb 22 2016 11:51:09.153 EDT: %SEC-6-IPACCESSLOGP: list 185 denied  
tcp 172.16.1.49(36426) -> 192.168.2.1(438), 1 packet [0x279C8521]
```

The screenshot shows a Notepad window with Cisco router logs. Numbered callouts identify the following fields:

- 1: Event ID (002416)
- 2: Date (Feb 22 2016)
- 3: Time (11:51:07.149 EDT)
- 4: Identifier (%SEC-6-IPACCESSLOGP)
- 5: Protocol applied (tcp)
- 6: Source IP address (172.16.1.14)
- 7: Destination IP address (192.168.2.1)


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In the above slide, there is a screenshot containing LOGS with the details such as event ID, data, time, identifier, protocol applied, source IP address, and destination IP address. Based on the Identifier that is (4) in the log sheet, the severity of the log is figured out at the time of analyzing security-related incidents.

Source: <http://www.cisco.com>



# Analyzing Router Logs: Juniper



- Juniper networking devices run on the company's proprietary **Junos operating system**
- The router stores logs in the **default messages file**
- In M-, MX-, and T-series routers, the log files are present in **/var/log/ location**
- In J-series routers, the log file location is **/cf/var/log/**
- Command to view the logs: **user@my-device > show log messages**
- The OS complies with **syslog severity level standards**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

JUNOS is an operating system that runs on the Juniper networking devices. The operating system provides two functionalities:

- **System logging**

System logging generates syslog messages that record the events in a router pertaining to logins, login failures, unexpected termination of the peer process, and router shutdowns in case of excess heat.

- **Tracing**


Tracing is mainly concerned with routing protocols. It stores all the information pertaining to its operations; exchange of packets during the start of a process or transferring the scheduled updates.

The above functions save the log messages to files. The logs of a Juniper router are by default saved in the file named **messages**. The router stores logs of messages to files. The log files are stored in the **/var/log/ location**, and the path is same for M-, MX-, and T-series router, for J-series routers the files are stored in is **/cf/var/log/**.

To view the logs, the following command can be used: **user@my-device > show log messages**

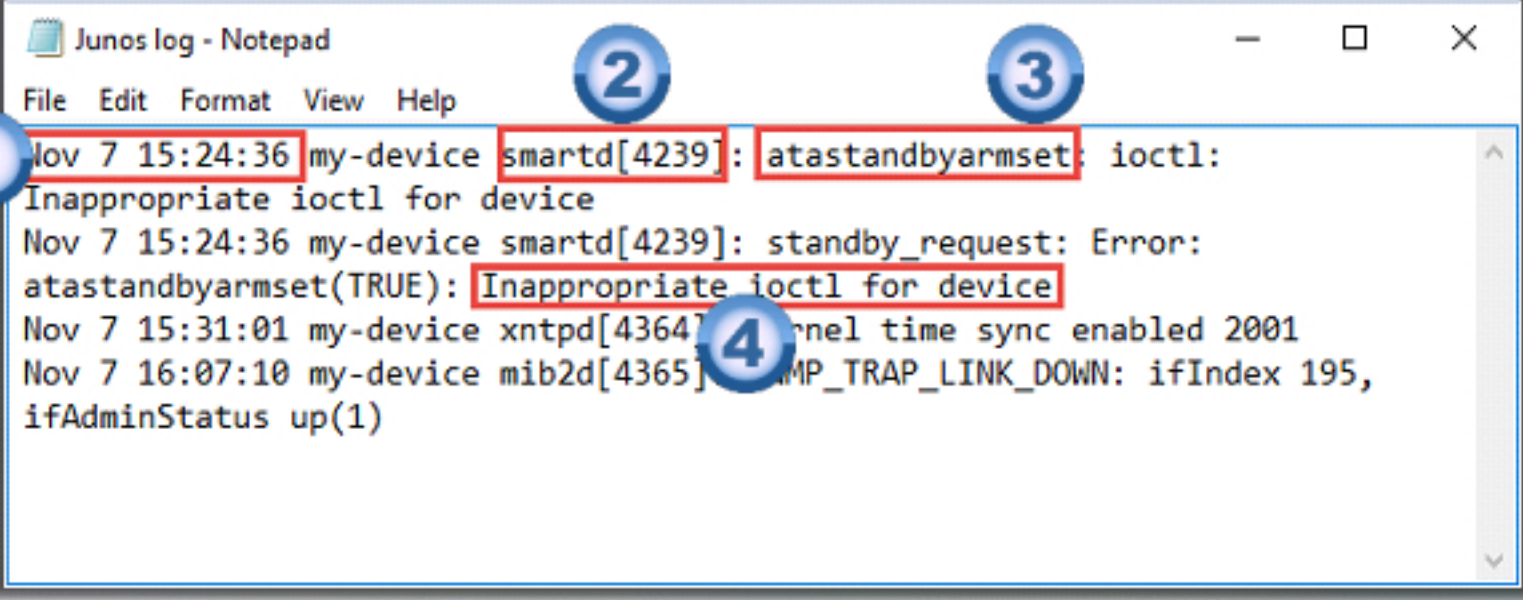



## Analyzing Router Logs: Juniper (Cont'd)



Juniper router logs include the following details:

1. Router name and ID
2. Status
3. Message
4. Date and Time

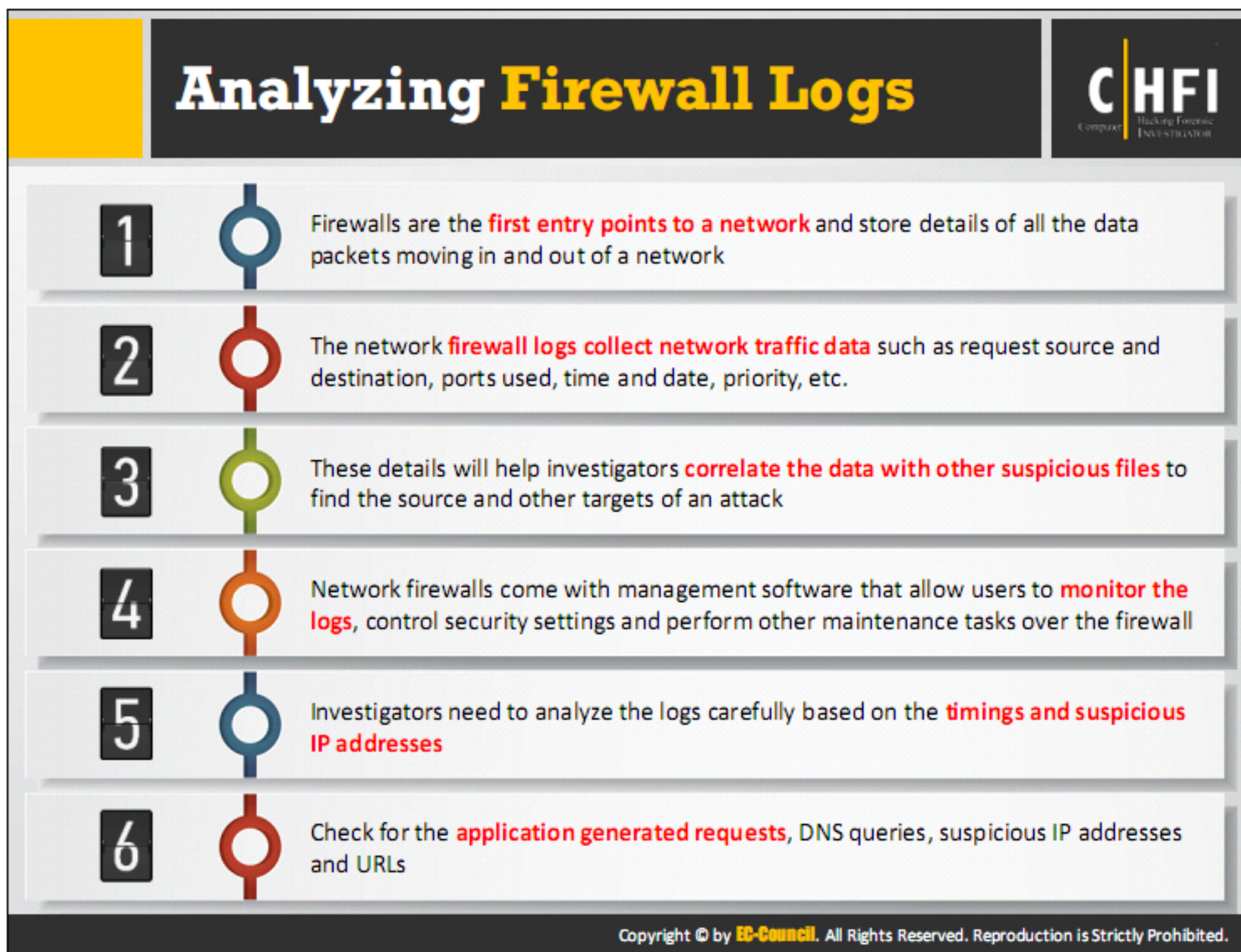


```
Junos log - Notepad
File Edit Format View Help
Nov 7 15:24:36 my-device smartd[4239]: atastandbyarmset: ioctl:
Inappropriate ioctl for device
Nov 7 15:24:36 my-device smartd[4239]: standby_request: Error:
atastandbyarmset(TRUE): Inappropriate ioctl for device
Nov 7 15:31:01 my-device xntpd[4364]: ntp time sync enabled 2001
Nov 7 16:07:10 my-device mib2d[4365]: SNMP_TRAP_LINK_DOWN: ifIndex 195,
ifAdminStatus up(1)
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In the above slide, there is a screenshot of a Juniper logfile. The log file contains date and time, router name and ID, status and message. In case of security breaches, investigators can use these details during log analysis.





A firewall is software or hardware that helps prevent hackers and few kinds of malware from getting to any PC through a network or the Internet. The file does this by checking the info that is coming from the Internet or a network and then either blocking it or allowing it to pass through to the PC.

The Firewall log file can be useful for determining the cause of program failures. The investigators can use logs to identify malicious activity, although the firewall does not provide the complete information needed to track down the source of the activity but provides a few insights about the nature of the activity.


The log is a plaintext file and can be viewed using any text editor. Notepad is the default text editor for the most Firewall log files. The period up to which the logs are stored depends on the storage limit set for the file. The newer logs replace older ones. The database administrators collect and store the logs from time to time due to the memory constraint.

During the time of security attacks, these logs can give the investigators an idea about the breach. The investigators can correlate these logs with other suspicious files to detect the source and other targets of the attack.

Source: <http://www.microsoft.com>



## Analyzing Firewall Logs: Cisco



■ Cisco Firewall uses mnemonics as identifiers to represent severity of any event

Mnemonic	Severity	Description
4000nn	4	PS:number string from IP_address to IP_address on Interface Interface_name
106001	2	Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on Interface Interface_name
106002	2	protocol Connection denied by outbound list acl_ID src Inside_address dest outside_address
106006	2	Deny Inbound UDP from outside_address/outside_port to Inside_address/Inside_port on Interface Interface_name
106007	2	Deny Inbound UDP from outside_address/outside_port to Inside_address/Inside_port due to DNS (Response Query)
106010	3	Deny Inbound protocol src Interface_name:dest_a ddress/dest_port dst
106012	3	Deny IP from IP_address to IP_address, IP options hex
106013	3	Dropping echo request from IP_address to PAT address IP_address
106014	3	Deny Inbound icmp src Interface_name: IP_address dst Interface_name: IP_address (type dec, code dec)
106015	6	Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on Interface Interface_name
106016	2	Deny IP spoof from (IP_address) to IP_address on Interface Interface_name.
106017	2	Deny IP due to Land Attack from IP_address to IP_address
106018	2	ICMP packet type ICMP_type denied by outbound list acl_ID src Inside_address dest outside_address
106020	2	Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
106021	1	Deny protocol reverse path check from source_address to dest_address on Interface Interface_name
106022	1	Deny protocol connection spoof from source_address to dest_address on Interface Interface_name
106023	4	Deny protocol src [Interface_name:source_address/source_port] dst Interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID
106100	4	access-list acl_ID {permitted   denied   est-allowed} protocol Interface_name/source_address(source_port) -> Interface_name/dest_a ddress(dest_port) hit+cnt number ((first hit   number-second interval))
710003	3	{TCP UDP} access denied by ACL from source_IP/source_port to Interface_name:dest_IP/service

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

In one way or the other, log messages are very useful; in most cases, a small subset of log messages will initially provide the most benefit. After examining these events, investigators can expand the scope of their analysis by searching for additional details. The below table summarizes the most common messages and the associated severity level. Fortunately, most of these messages come from fairly contiguous mnemonic identifiers. The Identifiers aid in identification when using command-line tools.

Source: <http://www.cisco.com>



## Analyzing Firewall Logs: Cisco (Cont'd)



Cisco firewall logs include the following details:

1. Date and Time
2. Mnemonic message
3. Firewall Action
4. Source IP address and port
5. Destination IP address and port
6. Type of request

```
Feb 24 2016 09:14:54: %ASA-6-106100: access-list OUTSIDE denied tcp outside/192.168.208.63  
(38807) -> inside/192.168.150.77(80) hit-cnt 1 first hit [0x22e8ac21, 0x0]  
Feb 24 2016 09:16:14: %ASA-6-106015: Deny TCP (no connection) from 192.168.150.65/2278 to  
64.101.128.83/80 flags RST on interface inside  
Feb 24 2016 09:16:41: %ASA-4-106023: Deny icmp src outside:192.168.208.63 dst  
inside:192.168.150.77 (type 8, code 0) by access-group "OUTSIDE" [0xd3f63b90, 0x0]  
Feb 24 2016 09:16:41: %ASA-6-106100: access-list OUTSIDE denied tcp outside/192.168.208.63  
(38664) -> inside/192.168.150.77(80) hit-cnt 1 first hit [0x22e8ac21, 0x0]  
Feb 24 2016 09:16:43: %ASA-4-106023: Deny icmp src outside:192.168.208.63 dst  
inside:192.168.150.77 (type 8, code 0) by access-group "OUTSIDE" [0xd3f63b90, 0x0]  
Feb 24 2016 09:16:43: %ASA-6-106100: access-list OUTSIDE denied tcp outside/192.168.208.63  
(38665) -> inside/192.168.150.77(80) hit-cnt 1 first hit [0x22e8ac21, 0x0]  
Feb 24 2016 09:17:32: %ASA-1-106021: Deny ICMP reverse path check from 192.168.150.60 to  
192.168.2.1 on interface outside
```


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Cisco firewall logs are in the above mentioned format. The logs contain date and time, mnemonic message, firewall action, source IP address and port, destination IP address and port, type of request. All these objects are useful to the investigators in the investigation process. From the below screenshot the Mnemonic can be identified from the table 3. With the help of Mnemonics the severity of the can be figured out.














Source: <http://www.cisco.com>



## Analyzing Firewall Logs: Checkpoint



- Checkpoint Firewall logs **can be viewed through a Check Point Log viewer** that uses icons and colors in the log table to represent different security events and their severity
- Red** represents the **connection attempts blocked by firewall** in accordance with the security policy or user-defined rules
- Orange** signifies **traffic detected** as suspicious, but accepted by the firewall
- Green** color is for the **traffic accepted by the firewall**
- Icons used in checkpoint logs include:

Action	Icon	Description
Connection Accepted		The firewall accepted a connection
Connection Decrypted		The firewall decrypted a connection
Connection Dropped		The firewall dropped a connection
Connection Encrypted		The firewall encrypted a connection
Connection Rejected		The firewall rejected a connection
Connection Monitored		A security event was monitored; however, it was not blocked, due to the current configuration
URL Allowed		The firewall allowed a URL
URL Filtered		The firewall blocked a URL
Virus Detected		A virus was detected in an email
Potential Spam Stamped		An email was marked as potential spam
Potential Spam Detected		An email was rejected as potential spam
Mail Allowed		A non-spam email was logged
Blocked by VStream Antivirus		VStream Antivirus blocked a connection

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Use the application Check Point Log viewer to view the checkpoint firewall logs. The application uses color coding to differentiate error severity, as mentioned in the table below (Table 4).

Event Log Color coding	
Red	An error message
Orange	A warning message
Blue	An information

TABLE 7.1: Eventlog color coding in checkpoint firewall log

ICONS represent every action in a Checkpoint firewall log viewer, as shown in the slide.



# Analyzing Firewall Logs: Checkpoint (Cont'd)



01

Checkpoint firewall log when viewed through Check Point Log viewer displays the result as follows


The screenshot shows the 'localhost - Check Point Log Viewer - [fw.log]' window. It contains a table of log entries with columns: Origin, Action, Service, Source, Destination, P., R., S., and Info. The entries include IKE logs, ICMP traffic, and various TCP connections, some of which are dropped.

Origin	Action	Service	Source	Destination	P.	R.	S.	Info.
192.168.0.122	key install		192.168.0.122	192.168.0.115				IKE Log: Phase 1 (aggressive) completion. 3DES/MD5/Pre shared secrets Negotiation id: 61893c3
192.168.0.122	key install		192.168.0.122	192.168.0.115	ip	0		scheme: IKE methods: Combined ESP; 3DES + MD6 (phase 2 completion) for subnet: 172.17.0.0 (
192.168.0.122	decrypt		172.16.0.100	172.17.0.12	icmp	3		icmp-type 8 icmp-code 0 scheme: IKE methods: Combined ESP; 3DES + MD5
192.168.0.122	encrypt		172.17.0.12	172.16.0.100	icmp	3		icmp-type 0 icmp-code 0 scheme: IKE methods: Combined ESP; 3DES + MD5
192.168.0.122	decrypt	webmin10000	172.16.0.100	172.17.0.12	tcp	3	1093	scheme: IKE methods: Combined ESP; 3DES + MD5
192.168.0.122	decrypt	webmin10000	172.16.0.100	172.17.0.12	tcp	3	1094	scheme: IKE methods: Combined ESP; 3DES + MD5
192.168.0.122	drop	bootpc	192.168.0.2	255.255.255.255	udp	7	bootp	len 328
192.168.0.122	accept	IKE	192.168.0.115	192.168.0.122	udp	2	IKE	len 288
192.168.0.122	key install		192.168.0.115	192.168.0.122	ip	0		scheme: IKE methods: Combined ESP; 3DES + MD6 + PFS (phase 2 completion) for subnet: 172.16
192.168.0.122	decrypt	webmin10000	172.16.0.100	172.17.0.12	tcp	3	1095	scheme: IKE methods: Combined ESP; 3DES + MD5
192.168.0.122	decrypt		172.16.0.100	172.17.0.12	icmp	3		icmp-type 8 icmp-code 0 scheme: IKE methods: Combined ESP; 3DES + MD5
192.168.0.122	encrypt		172.17.0.12	172.16.0.100	icmp	3		icmp-type 0 icmp-code 0 scheme: IKE methods: Combined ESP; 3DES + MD5
192.168.0.122	drop	bootpc	192.168.0.2	255.255.255.255	udp	7	bootp	len 328




Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



# Analyzing IDS Logs



- IDS Logs provide information helpful in finding **suspicious packet** types, determining the probes, generating new attack signatures and measuring attack statistics
- Most common **IDS devices** include **Juniper** and **Checkpoint**
- General indicators** of intrusion:

Requests targeted towards known vulnerabilities		Repeated unusual network activity
Failure to comply with protocols and syntaxes		Address anomalies in traffic
Unexpected elements such as date, time, system resources, etc.		Occurrence of mistyped command

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

In addition to monitoring and analyzing events to identify undesirable activity, all types of IDS technologies typically perform the following functions:

- **Recording information related to observed events:** IDS usually records Information locally and sends this information to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.
- **Notifying security administrators:** The IDS alerts the network security administrators through e-mails, pages, messages on the IDS user interface, simple network management protocol (SNMP) traps, system log messages, and user-defined programs and scripts.
- **Producing reports:** The IDS offers reports that summarize the monitored events or provides details on specific events of interest.



# Analyzing IDS Logs: Juniper



- Juniper IDS comes with in-built Network and Security Manager (NSM), which stores event logs
- Users need the NSM log viewer to view and analyze the logs
- Juniper IDS stores logs with the information mentioned in the table



Column	Description
Log ID	Unique ID for the log entry, derived by combining the date and log number.
Time Received	Date and time that the management system received the log entry.
Alert	NSM-defined alert for this type of log entry. Configure alerts in policy rules.
User Flag	To set a flag, right-click the log row, select Flag, and then select one of the following flags from high, medium, low, closed, false positive, assigned, investigate, follow-up, pending
Src Addr	Source IP address of the packet that generated the log entry.
Dst Addr	Destination IP address of the packet that generated the log entry.
Action	Action the security device performed on the packet/connection that generated this log entry: •Accepted—Did not block the packet. •Closed Client—Closed the connection and sent an RST packet to the client, but did neither to the server. •Closed Server—Closed the connection and sent an RST packet to the server, but did neither to the client. •Closed—Closed the connection and sent an RST packet to both the client and the server. •Dropped—Dropped the connection without sending an RST packet to the sender, preventing the traffic from reaching its destination. •Dropped Packet—Dropped a matching packet before it could reach its destination but did not close the connection. •Ignored—Matched the attack, did not take action, and ignored the remainder of the connection.
Protocol	Protocol that the packet that generated the log entry used.
Dst Port	Destination port of the packet that generated the log entry.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Analyzing IDS Logs: Juniper (Cont'd)



Rule #	Security policy rule that generated the log entry.
Nat Src Addr	NAT source address of the packet that generated the log entry.
Nat Dst Addr	NAT destination address of the packet that generated the log entry.
Details	Miscellaneous string associated with log entry.
Category	Type of log entry: •Admin •Alarm—The device generates event alarms for any security event that has a predefined severity level of emergency, critical, or alert. Additionally, the device generates traffic alarm log entries when it detects network traffic that exceeds the specified alarm threshold in a rule (the traffic alarm log entry describes the security event that triggered the alarm). •Config—A configuration change occurred on the device. •Custom—A match with a custom attack object was detected. •Implicit—An implicit rule was matched. •Info—General system information. •Predefined—A match with a predefined attack object was detected. •Profiler—Traffic matches a Profiler alert setting. •Screen—Not applicable for IDP Series devices. Generated by ScreenOS firewall devices. •Self—The device generated this log for a non-traffic related reason. •Sensor. •Traffic—Traffic matches a rule you have configured for harmless traffic. •URL Filtering—Not applicable for IDP Series devices. Generated by ScreenOS firewall devices. •User.
Subcategory	Category-specific type of log entry (examples are "Reboot" or message ID).

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Analyzing IDS Logs: Juniper (Cont'd)



Severity	Severity rating associated (if any) with this type of log entry: <ul style="list-style-type: none"><li>• Not Set (the device could not determine a severity for this log entry)</li><li>• Info</li><li>• Device_warning_log</li><li>• Minor and Major</li><li>• Device_critical_log</li><li>• Emergency</li><li>• Error</li><li>• Notice</li><li>• Informational</li><li>• Debug</li></ul>
Device	Device that generated this log entry.
Comment	User-defined comment about the log entry.
Application Name	Application associated with the current log.
Bytes In	For sessions, specifies the number of inbound bytes.
Bytes Out	For sessions, specifies the number of outbound bytes.
Bytes Total	For sessions, specifies the combined number of inbound and outbound bytes.
Dev Domain Ver	Domain version that generated this log entry.
Device Domain	Domain for the device that generated this log entry.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Analyzing IDS Logs: Juniper (Cont'd)




Device family	Family of the device that generated this log entry.
Dst Intf	Name of the outbound interface of the packet that generated this log entry.
Dst Zone	Destination zone associated with a traffic log entry.
Elapsed Secs	For sessions, specifies how long the session lasted.
Has Packet Data	Indicates whether the log entry has associated packet data.
NAT Dst Port	The NAT destination port of the packet that generated the log entry.
NAT Src Port	The NAT source port of the packet that generated the log entry.
Packets In	For sessions, specifies the number of inbound packets.
Packets Out	For sessions, specifies the number of outbound packets.
Packets Total	For sessions, specifies the combined number of inbound and outbound packets.
Policy	Security policy that generated the log entry.
Roles	Role group associated with this log entry.
Rule Domain	The domain of the rule that generated the log entry.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Analyzing IDS Logs: Juniper (Cont'd)



Rule Domain Ver	The domain version of the rule that generated the log entry.
Rulebase	Security policy rulebase that generated the log entry.
Src Intf	Name of the inbound interface of the packet that generated this log entry.
Src Port	Source port of the packet that generated the log entry.
Src Zone	Source zone associated with a traffic log entry.
Time Generated	Date and time the device generated the log entry.
User	User associated with this log entry.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In Juniper IDS, the system logs events when it reaches the rising and reset threshold for memory usage, CPU usage, disk space usage, or maximum number of active sessions, as per default. The default threshold is 90%; however, you can optionally configure logging for other operational events such as flow or fragment errors.

The event logs of Juniper IDS are stored in the Network and Security Manager (NSM), which is in-built in the device. NSM log viewer is used to view and analyze the logs. Juniper IDS store logs with the information with the objects mentioned in the table.

Source: <https://www.juniper.net>



## Analyzing IDS Logs: Juniper (Cont'd)



Details provided by the IDS in logs include:

1. Date and Time
2. Device IP address
3. Attack type
4. Source Address
5. Source Port
6. Destination Address
7. Severity of the attack

```
<26> 1 2016-01-30T15:48:54 10.60.0.208 Jnpr Syslog 30297 1 [syslog@juniper.net
dayId="20160130" recordId="0" timeRecv="2016/01/30 15:48:54"
timeGen="2016/01/30 15:48:54" domain="" devDomVer2="0" device ip="10.60.0.208"
cat="Predefined" attack="HTTP:XSS:HTML-SCRIPT-IN-URL-PR" srcZn="NULL" srcIntf="
eth1" srcAddr="192.168.33.24" srcPort="1495" dstSrcAddr="NULL" natSrcPort="0"
dstZ 4 "NULL" dstIntf="NULL" dstAddr="192.168.33.1" dstPort="80"
natDstAddr="NULL" natDstPort 6 "0" protocol="TCP" ruleDomain="" ruleVer="0"
policy="Recommended" rulebase="IDS" ruleNo="3" action="DROP" severity="MAJOR"
alert="no" elapsedTime="0" inbytes="0" outbytes="0" totByte 7 "0" inPak="0"
outPak="0" totPak="0" repCount="0" packetData="no" varEnum="31"
misc="`interface=eth1` user=NULL app=NULL uri=NULL"]]
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The IDS logs include contains date and time, device IP address, attack type, source address, source port and destination address and the severity of the attack. These objects help the investigators in the investigation proceed further. Table 8 informs about the severity of the attack mentioned in the LOG.



## Analyzing IDS Logs: Checkpoint



- Checkpoint IPS has an **in-built software** for managing the device
- Users can view and analyze the logs using this software
- Steps to view and access logs in **checkpoint IDS**:
  - Go to SmartDashboard, click **SmartConsole** → select **SmartView Tracker**
  - Select the **Network & Endpoint** tab, expand **Predefined** → **Network Security Blades** → **IPS Blade**
  - Double-click **All** to view the complete **log information**

N.	Y.	Date	Time	Source	Source User Name	Destination	Attack	Attack Information
1	28Dec2008	11:11:11	10.0.112.7	Thomas Harris (tharris)	10.0.154.60		Web Client Enforcement Violati...	Microsoft Word structure process...
2	28Dec2008	11:11:11	10.0.204.181	Evans Smith (esmith)	10.0.21.102		Web Client Enforcement Violati...	OIE Automation remote code exec...
3	28Dec2008	11:11:11	10.0.99.215	Freddy Baker (fbaker)	10.0.215.168		Peer to Peer	BitTorrent protocol detected on co...
4	28Dec2008	11:11:11	10.0.217.151	Lisa Smith (lsmith)	10.0.140.94		Non Compliant MSSQL TCP	Parsing Error - Cannot Recognize T...
5	28Dec2008	11:13:39	10.0.191.243	Thomas Harris (tharris)	10.0.196.177		Non Compliant DNS	Bad DNS header
6	28Dec2008	11:16:42	10.0.39.176		10.0.90.245		Non Compliant MSSQL TCP	Parsing Error - Cannot Recognize T...
7	28Dec2008	11:22:03	10.0.110.173	Evans Smith (esmith)	10.0.122.77		Peer to Peer	BitTorrent protocol detected on co...
8	28Dec2008	11:22:12	10.0.244.79	Freddy Baker (fbaker)	10.0.214.94		Web Client Enforcement Violati...	Microsoft Word RTF Object Parsin...
9	28Dec2008	11:22:57	10.0.119.66	Lisa Smith (lsmith)	10.0.40.204		Web Client Enforcement Violati...	Visual Studio WMI code execution ...
10	28Dec2008	11:23:30	10.0.139.166	Thomas Harris (tharris)	10.0.145.229		Web Client Enforcement Violati...	Microsoft Word structure process...
11	28Dec2008	11:23:38	10.0.253.84	Lisa Smith (lsmith)	10.0.141.127		Web Client Enforcement Violati...	Microsoft Word RTF Object Parsin...
12	28Dec2008	11:25:09	10.0.186.139	Evans Smith (esmith)	10.0.124.127		Non Compliant DNS	Bad DNS header
13	28Dec2008	11:29:43	10.0.47.78	Lisa Smith (lsmith)	10.0.94.33		Web Client Enforcement Violati...	OIE Automation remote code exec...
14	28Dec2008	11:32:01	10.0.168.128	Thomas Harris (tharris)	10.0.173.41		QQ Instant Messenger	QQ Instant Messenger Blocked
15	28Dec2008	11:35:39	10.0.12.217	Lisa Smith (lsmith)	10.0.151.120		Non Compliant DNS	Bad DNS header
16	28Dec2008	11:36:11	10.0.73.198	Evans Smith (esmith)	10.0.176.24		Web Client Enforcement Violati...	Microsoft Word RTF Object Parsin...

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The in-built software can be used to manage the device, Checkpoint IPS. The users can view and analyze the logs using this software.

Steps to view and access logs in checkpoint IDS are as follows:


- Go to SmartDashboard, click SmartConsole → select SmartView Tracker
- Select the Network & Endpoint tab, expand Predefined> Network Security Blades> IPS Blade
- Double-click All to view the complete log information

The events log displays all events generated by the IPS Blade, including information about the data, the protection, and the action taken.

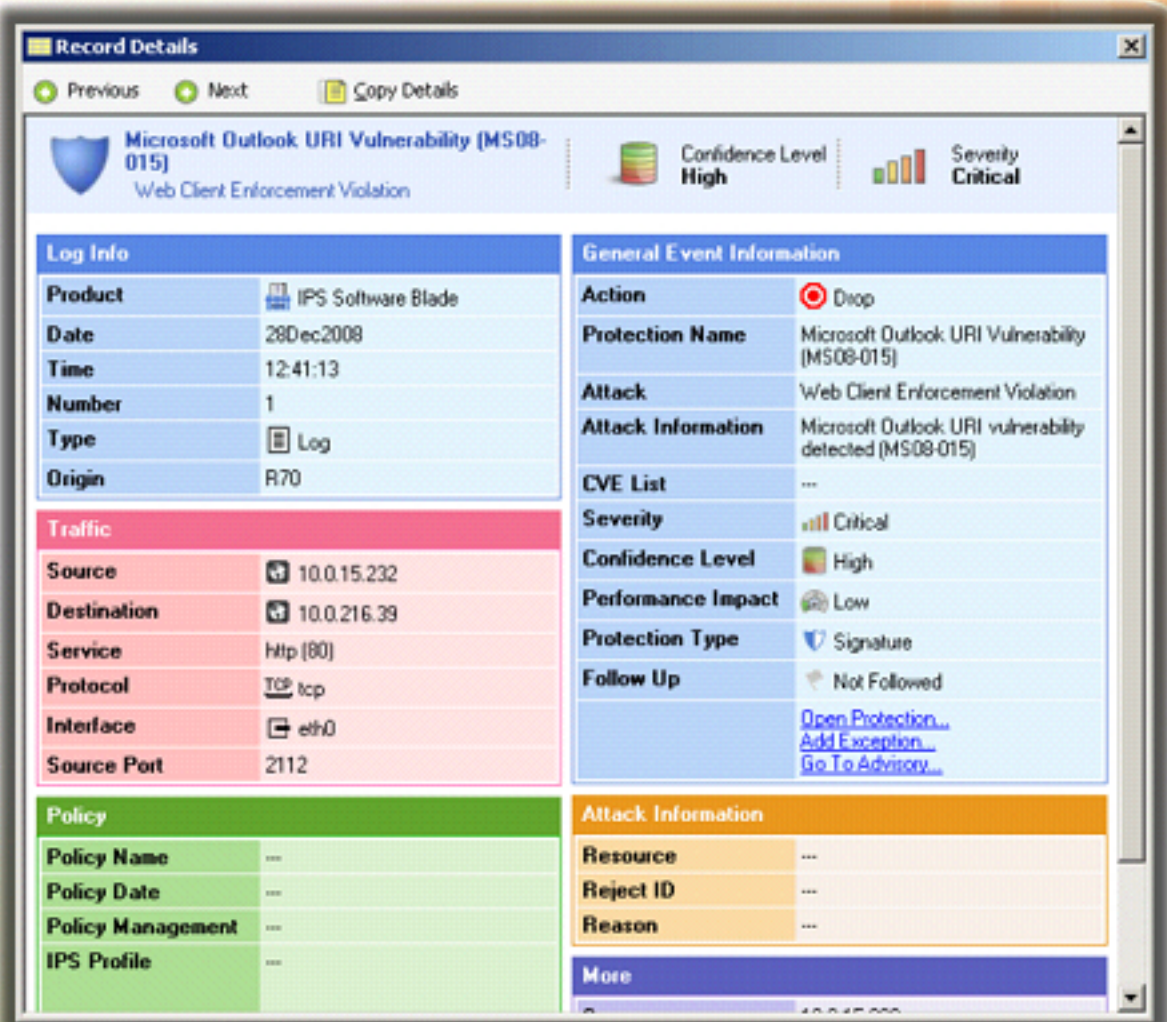
Source: <https://sc1.checkpoint.com>



## Analyzing IDS Logs: Checkpoint (Cont'd)



- Checkpoint IPS also provides details of each log
- To view the details of any log, go to the SmartView Tracker records list and double-click on the event



The screenshot shows the 'Record Details' window for a Microsoft Outlook URI Vulnerability (MS08-015) event. The window is divided into several sections:

- Log Info:** Product (IPS Software Blade), Date (28Dec2008), Time (12:41:13), Number (1), Type (Log), Origin (R70).
- Traffic:** Source (10.0.15.232), Destination (10.0.216.39), Service (http (80)), Protocol (TCP), Interface (eth0), Source Port (2112).
- Policy:** Policy Name, Policy Date, Policy Management, IPS Profile.
- General Event Information:** Action (Drop), Protection Name (Microsoft Outlook URI Vulnerability (MS08-015)), Attack (Web Client Enforcement Violation), Attack Information (Microsoft Outlook URI vulnerability detected (MS08-015)), CVE List, Severity (Critical), Confidence Level (High), Performance Impact (Low), Protection Type (Signature), Follow Up (Not Followed).
- Attack Information:** Resource, Reject ID, Reason.


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Check Point logs provides information of the network traffic to allow adjustment of the bandwidth. Analyzing the logs is very important for business risk valuation.

Checkpoint IPS provides details of each log. The details of any log can be accessed by going to the Smart View Tracker records list and double-clicking on the event.



# Analyzing Honeypot Logs

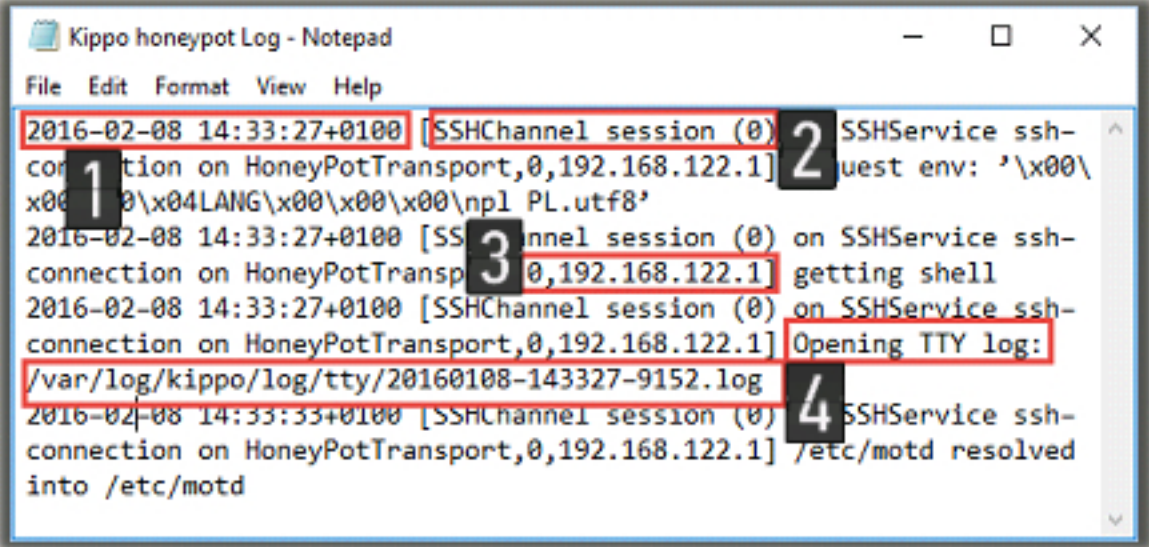


**01** Honeypots are the devices that pretend to contain very useful information in order to lure attackers and find their whereabouts and techniques

**02** Kippo is one of the most commonly used honeypots

**03** Logs stored in Kippo contain the following information:

- 1. Timestamp
- 2. Type of session
- 3. Session ID and Source IP address
- 4. Message with other details



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Honeypots are deception traps that are designed such that they attract the attackers to compromise the information systems in a group. The honeypots are the dummy systems used to understand the strategies of the attackers and protect the organization from the attacks.

Kippo is one of the commonly used Honeypots to fool the attackers and understand their methodology thereby minimizing the risk of attack.



# DHCP Logging



- The DHCP logs are saved in the **C:\Windows\System32\dhcp** folder on **DHCP servers**
- DHCP server log file format**
  - ID, Date, Time, Description, IP Address, Host Name, MAC Address



Field	Description
ID	A DHCP Event ID code
Date	The date on which this entry was logged on the DHCP server
Time	The time at which this entry was logged on the DHCP server
Description	A description of this DHCP server event
IP Address	The IP address of the DHCP client
Host Name	The host name of the DHCP client
MAC Address	The media access control (MAC) address used by the network adapter hardware of the client

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Sample DHCP Audit Log File



```
DhcpSrvLog-Mon - Notepad
File Edit Format View Help
Microsoft DHCP Service Activity Log

Event ID Meaning
00 The log was started.
01 The log was stopped.
02 The log was temporarily paused due to low disk space.
10 A new IP address was leased to a client.
11 A lease was renewed by a client.
12 A lease was released by a client.
13 An IP address was found to be in use on the network.
14 A lease request could not be satisfied because the scope's address pool was exhaust
15 A lease was denied.
16 A lease was deleted.
17 A lease was expired and DNS records for an expired leases have not been deleted.
18 A lease was expired and DNS records were deleted.
20 A BOOTP address was leased to a client.
21 A dynamic BOOTP address was leased to a client.
22 A BOOTP request could not be satisfied because the scope's address pool for BOOTP w
23 A BOOTP IP address was deleted after checking to see it was not in use.
24 IP address cleanup operation has began.
25 IP address cleanup statistics.
30 DNS update request to the named DNS server.
31 DNS update failed.
32 DNS update successful.
33 Packet dropped due to NAP policy.
34 DNS update request failed.as the DNS update request queue limit exceeded.
35 DNS update request failed.
50+ Codes above 50 are used for Rogue Server Detection information.

QResult: 0: NoQuarantine, 1:Quarantine, 2:Drop Packet, 3:Probation,6:No Quarantine Informat
ID,Date,Time,Description,IP Address,Host Name,MAC Address,User Name, TransactionID, QResult
00,05/07/12,13:27:39,Started,,,,,0,6,,
```

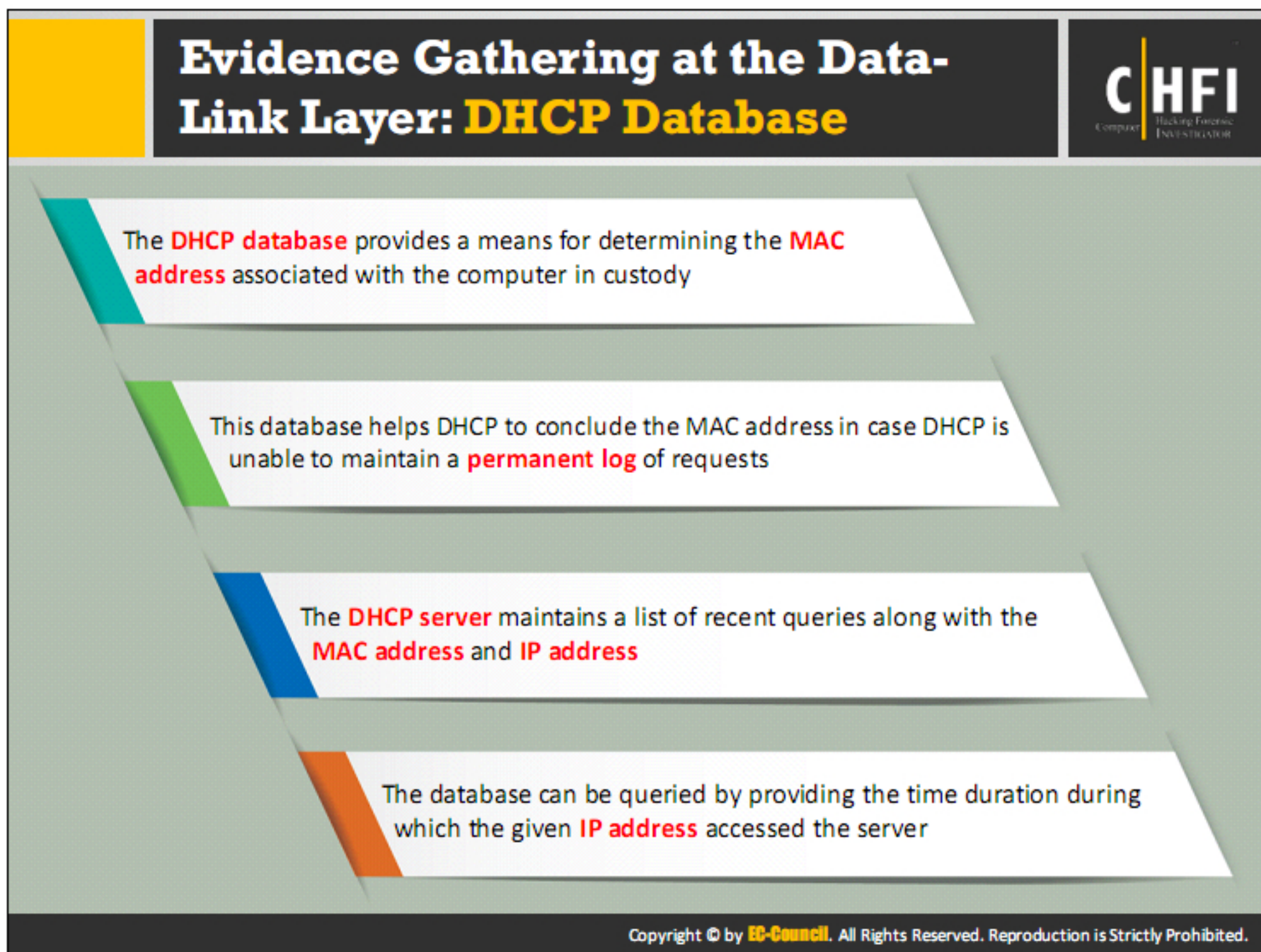
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



DHCP server in a network allocates IP address to a computer during its start up. Therefore, the DHCP server logs contain information regarding the systems that were assigned specific IP addresses by the server, at any given instance. Investigators can examine these logs during forensic examinations.

The `C:\Windows\System32\dhcp` folder on DHCP servers stores the DHCP logs, while the `C:\Windows\system32\dhcp\backup` folder contains a backup of the `dhcp` folder. DHCP server log file format includes fields for ID, date, time, description, IP address, host name, and MAC Address.





The DHCP database provides a means for determining the MAC addresses associated with the computer in custody. This database helps DHCP to conclude the MAC address in case DHCP is unable to maintain a permanent log of the single request received.

The DHCP server maintains a list of recent queries along with the MAC address and IP address. Investigators can query the database by giving the time duration during which the given IP address accessed the server.


Investigators can also refer the ARP table during an investigation to determine the MAC addresses. The ARP table maintained on the router is of crucial importance, as it can provide information about the MAC address of all the hosts involved in the recent communication.

Investigators can document the ARP table by any of the following means:

- Taking a photograph of the computer screen
- Taking a screenshot of the table and saving it on the disk
- Using the HyperTerminal logging facility



# ODBC Logging



Open Database Connectivity (ODBC) logging records a set of data fields in an ODBC-compliant database like Microsoft Access or Microsoft SQL Server

With ODBS logging, the administrator must specify both the database to be logged, and set up the database to receive the data

Some of logged information includes the user's IP address, user name, request date and time, HTTP status code, bytes received, bytes sent, action carried out, and the target file

When ODBC logging is enabled, IIS disables the HTTP.sys kernel-mode cache. This is the reason, implementing ODBC logging can degrade overall server performance

Field Name	SQL Server Field Type	MS Access Field Type
ClientHost	varchar(255)	text(255)
Username	varchar(255)	text(255)
LogTime	date time	date time
Service	varchar(255)	text(255)
Machine	varchar(255)	text(255)
ServerIP	varchar(50)	text(50)
ProcessingTime	int	int
BytesRecvd	int	int
BytesSent	int	int
ServiceStatus	int	int
Win32Status	int	int
Operation	varchar(255)	text(255)
Target	varchar(255)	text(255)
Parameters	varchar(255)	text(255)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

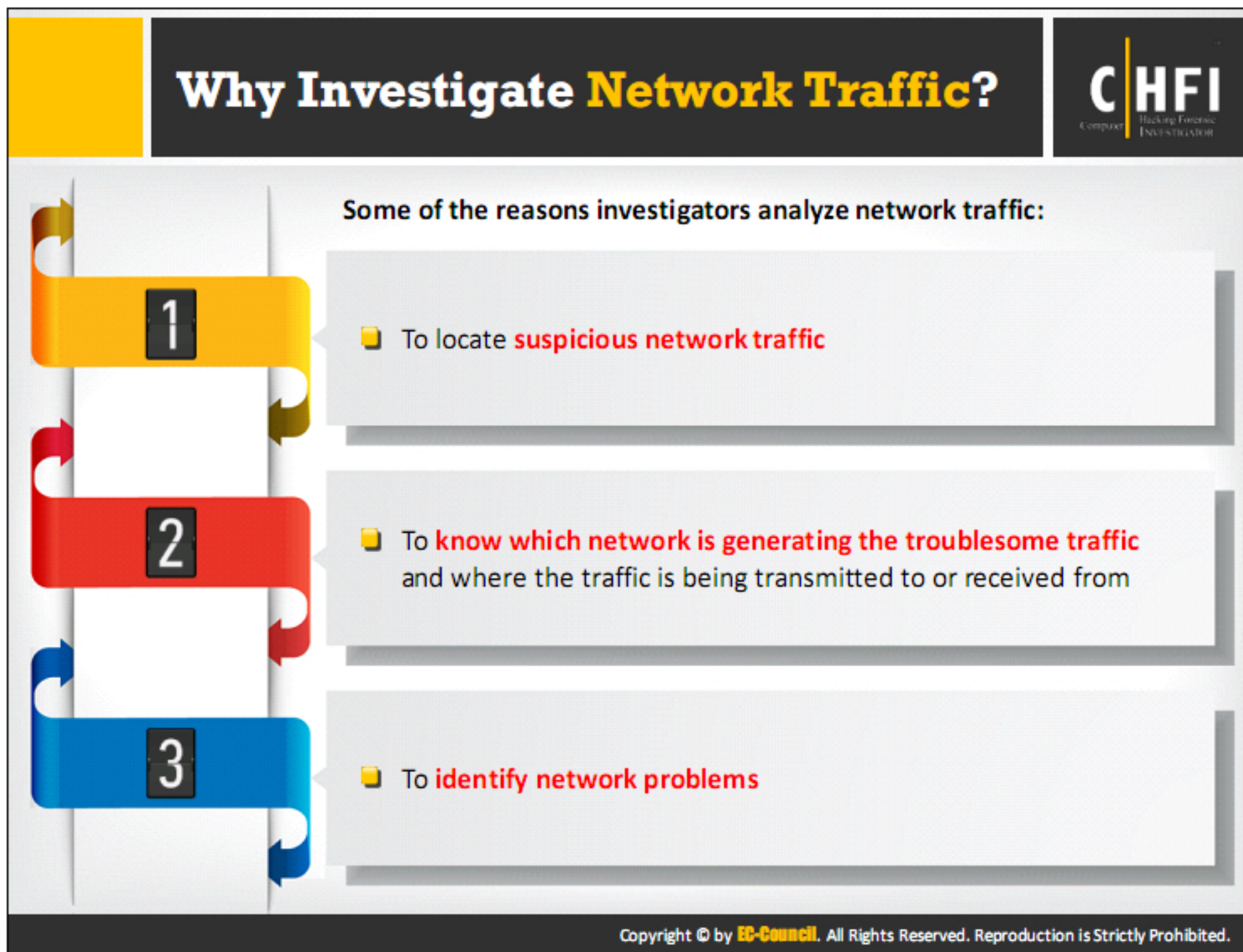
ODBC logging records a fixed set of data fields in an ODBC-compliant database, such as Microsoft Access or Microsoft SQL Server. With ODBC logging, a database must be set up to receive the data and this database must be specified to record the log files.

For computers running on SQL server, the IIS ODBC logging table can be created with a Transact-SQL script named logtemp.sql, which is included with IIS. Following are the steps to create ODBC logging table:

1. Log on to the server with a user account that has administrative access on the computer that is running SQL Server
2. Open SQL Server Query Analyzer
3. On the File menu, choose Open
4. Locate the %Windir%\System32\inetsrv folder
5. Select logtemp.sql and then, click Open
6. In the first line of the logtemp.sql script, replace inetlog with InternetLog
7. Select the database to create the InternetLog table. By default, the database is Master, but Microsoft does not recommend that you use this database
8. Click Query, and then click Execute

Source: <http://support.microsoft.com>





Investigating network traffic can help the administrator or the investigator to find out if the traffic is normal and abnormal. They can execute the following functions:

- Detect any suspicious activity within the environment and try to minimize the severity of the attack
- Identify and avoid security intrusions
- Detect if an attacker compromises a system and deletes files that only the network-based evidence can help the investigators for forensic analysis
- Identify suspicious activities
- Adjust bandwidth as per the usage.





A computer connected to the LAN has two addresses. One is the MAC address that specifically identifies each node in the network and is stored on the network card itself. The ethernet protocol uses the MAC address while building “frames” to exchange the data among the systems. The other is the IP address used by the applications. The data-link layer uses an ethernet header with the MAC address of the destination machine instead of the IP address. The network layer is responsible for mapping IP network addresses to the MAC address, as required by the data-link protocol. It initially looks for the MAC address of the destination machine in a table, usually called the ARP cache. An ARP broadcast of a request packet goes out to all machines on the local sub-network when no entry for the IP address can be found. The machine that has that particular address responds to the source machine with its MAC address and MAC address adds to the source machine’s ARP cache. The source machine then uses this MAC address in all its communications with the destination machine.

There are two basic types of ethernet environments, and sniffers work slightly differently in both of these environments. The two types of ethernet environments are shared ethernet and switched ethernet.



# Sniffing Tool: Wireshark

**CHFI**  
Computer Hacking Forensic Investigator

It lets you **capture and interactively browse the traffic** running on a computer network

01

Wireshark uses **Winpcap** to capture packets, therefore, it can only capture the packets on the networks supported by Winpcap

02

It **captures live network traffic** from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI networks

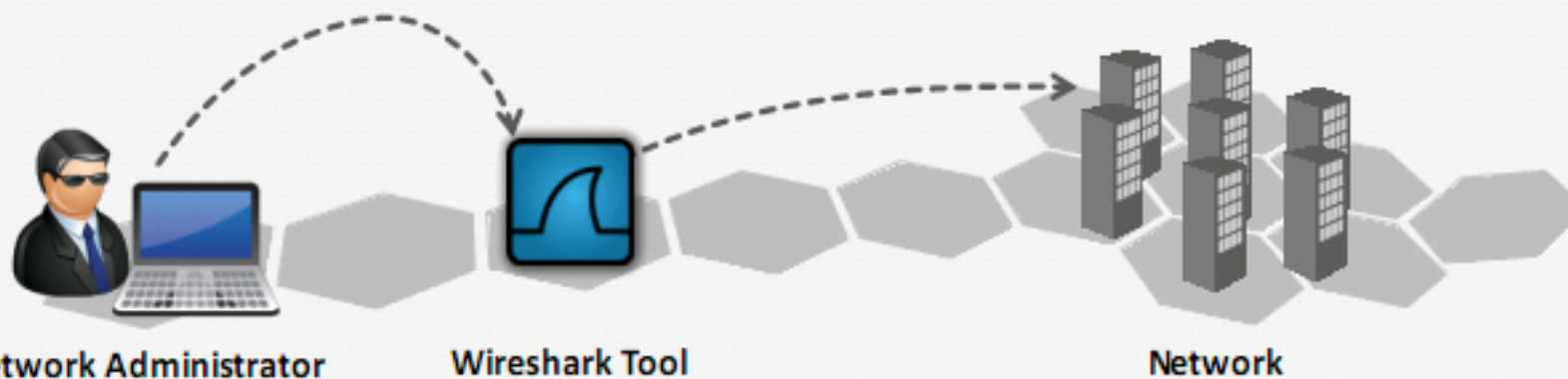
03

Captured files can be programmatically edited via **command-line**

04

A **set of filters** for customized data display can be refined using a display filter

05



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Sniffing Tool: Wireshark (Cont'd)

**CHFI**  
Computer Hacking Forensic Investigator

Filter:  Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.168.133	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
2	1.60276800	fe80::4855:5c3d:b13ff02::1:3		LLMNR	85	Standard query 0x4d7a A seot4
3	1.60342500	192.168.168.61	224.0.0.252	LLMNR	65	Standard query 0x4d7a A seot4
4	1.70272400	fe80::4855:5c3d:b13ff02::1:3		LLMNR	85	Standard query 0x4d7a A seot4
5	1.70272800	192.168.168.61	224.0.0.252	LLMNR	65	Standard query 0x4d7a A seot4
6	1.72908900	de11_c3:b1:8b	Broadcast	ARP		
7	1.72911900	cadmusco_73:24:9f	de11_c3:b1:8b	ARP		
8	1.72986900	192.168.168.75	192.168.168.133	TCP		
9	1.73001600	cadmusco_73:24:9f	Broadcast	ARP		
10	1.73067600	de11_c3:b1:8b	cadmusco_73:24:9f	ARP		
11	1.73069300	192.168.168.133	192.168.168.75	TCP		
12	1.73139200	192.168.168.75	192.168.168.133	TCP		
13	1.73178000	107.168.168.75	107.168.168.133	HTTP		

Frame 3: 65 bytes on wire (520 bits), 65 bytes captured (520 b)  
Ethernet II, Src: Elitegro\_22:30:de (00:25:11:22:30:de), Dst:  
Internet Protocol Version 4, Src: 192.168.168.61 (192.168.168.  
User Datagram Protocol, Src Port: 49279 (49279), Dst Port: 11  
Link-Local Multicast Name Resolution (query)

0000 01 00 5e 00 00 fc 00 25 11 22 30 de 08 00 45 00 ...A...  
0010 00 33 07 f3 00 00 01 11 67 e5 c0 a8 a8 3d e0 00 ...3...  
0020 00 fc c0 7f 14 eb 00 1f b1 d0 4d 7a 00 00 00 01 ...  
0030 00 00 00 00 00 00 05 73 65 6f 74 34 00 00 01 00 ...  
0040 01

Ethernet: <live capture in progress> File: C:\... Packets: 2194 - Displayed: 2194 (100.0%)

<http://www.wireshark.org>

Wireshark Filter Expression - Profile: Default

Field name	Relation	Value (Protocol)
104apci - IEC 60870-5-104-Apci	is present	
104asdu - IEC 60870-5-104-Asdu	==	
2dparityfec - Pro-MPEG Code of Practice #3 relea	!=	
3COMXNS - 3Com XNS Encapsulation	>	
3GPP2 A11 - 3GPP2 A11	<	
6LoWPAN - IPv6 over IEEE 802.15.4	>=	
802.11 MGT - IEEE 802.11 wireless LAN managem	<=	
802.11 Radiotap - IEEE 802.11 Radiotap Capture h	contains	
802.3 Slow protocols - Slow Protocols	matches	
9P - Plan 9 9P		
A-bis OML - GSM A-bis OML		
AAL1 - ATM AAL1		
AAL3/4 - ATM AAL3/4		

Range (offset:length)

OK Cancel

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Source: <http://www.wireshark.org>

Wireshark is a GUI network protocol analyzer. It lets the user interactively browse packet data from a live network or from a previously saved capture file. Wireshark's native capture file format is in libpcap format, which is also the format used by tcpdump and various other tools. In addition, Wireshark can read capture files from snoop and atmsnoop, Shomiti/Finisar Surveyor, Novell LANalyzer, Network General/Network Associates DOS-based Sniffer (compressed or uncompressed), Microsoft Network Monitor, and so on.

Wireshark does not require identification of the type of file the user is reading; it will determine the file type by itself. Wireshark is also capable of reading any file format that is compressed by using gzip. Wireshark recognizes this directly from the file; the .gz extension is not required for this purpose. Like other protocol analyzers, Wireshark's main window shows three views of a packet. It shows a summary line, briefly describing what the packet is. It shows a protocol tree allowing the user to drill down to the exact protocol, or field, that he or she is interested in. Finally, a hex dump shows the user exactly what the packet looks like when it goes over the wire.

In addition, Wireshark has other features. It can assemble all the packets in a TCP conversation and show the user the ASCII (or EBCDIC, or hex) data in that conversation. Display filters in Wireshark are very powerful. The pcap library performs packet capturing. The capture filter syntax follows the rules of the pcap library. This syntax is different from the display filter syntax.

Compressed file support uses the zlib library. If the zlib library is not present, Wireshark will compile, but will be unable to read compressed files. The -r option can be used to specify the path name for reading a captured file or to specify the path name as a command-line argument.

#### **Features include the following:**

- Allows browsing of captured network data
- Captures files compressed with gzip and can decompress them
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Enables exporting output to XML, PostScript, CSV, or plaintext

#### **Follow TCP Stream in Wireshark**

While working with TCP based protocols, it can be helpful to see the data from a TCP stream in the way that the application layer sees it if the investigator is looking for passwords in a Telnet stream or trying to make sense of a data stream. Only a display filter may be needed to show only the packets of that TCP stream. If so, Wireshark's ability to follow a TCP stream will be useful.

The user needs to simply select a TCP packet in the packet list of the appropriate stream/connection and then select the Follow TCP Stream menu item from the Wireshark Tools. Wireshark will set an appropriate display filter and pop up a dialog box with all the data from the TCP stream laid out in order, as shown in the below figure.



The stream content is displayed in the same sequence as it appeared on the network. Traffic from A to B is marked in red, while traffic from B to A is marked in blue. However the colors can be changed. These colors in the “Colors” page if the “Preferences” dialog.

Non-printable characters will be replaced by dots.

The stream content will not be updated while doing a live capture. To get the latest content, the user is required to reopen the dialog.

You can choose from the following actions:

**Save As:** Save the stream data in the currently selected format.

**Print:** Print the stream data in the currently selected format.

**Direction:** Choose the stream direction to be displayed (“Entire conversation”, “data from A to B only” or “data from B to A only”).

**Filter out this stream:** Apply a display filter removing the current TCP stream data from the display.

**Close:** Close this dialog box, leaving the current display filter in effect.

You can choose to view the data in one of the following formats:

**ASCII:** In this view you see the data from each direction in ASCII. Obviously best for ASCII based protocols, e.g. HTTP.

**EBCDIC:** For the big-iron freaks out there.

**HEX Dump:** This allows you to see all the data. This will require a lot of screen space and is best used with binary protocols.

**C Arrays:** This allows you to import the stream data into your own C program.

**Raw:** This allows you to load the unaltered stream data into a different program for further examination. The display will look the same as the ASCII setting, but “Save As” will result in a binary file.



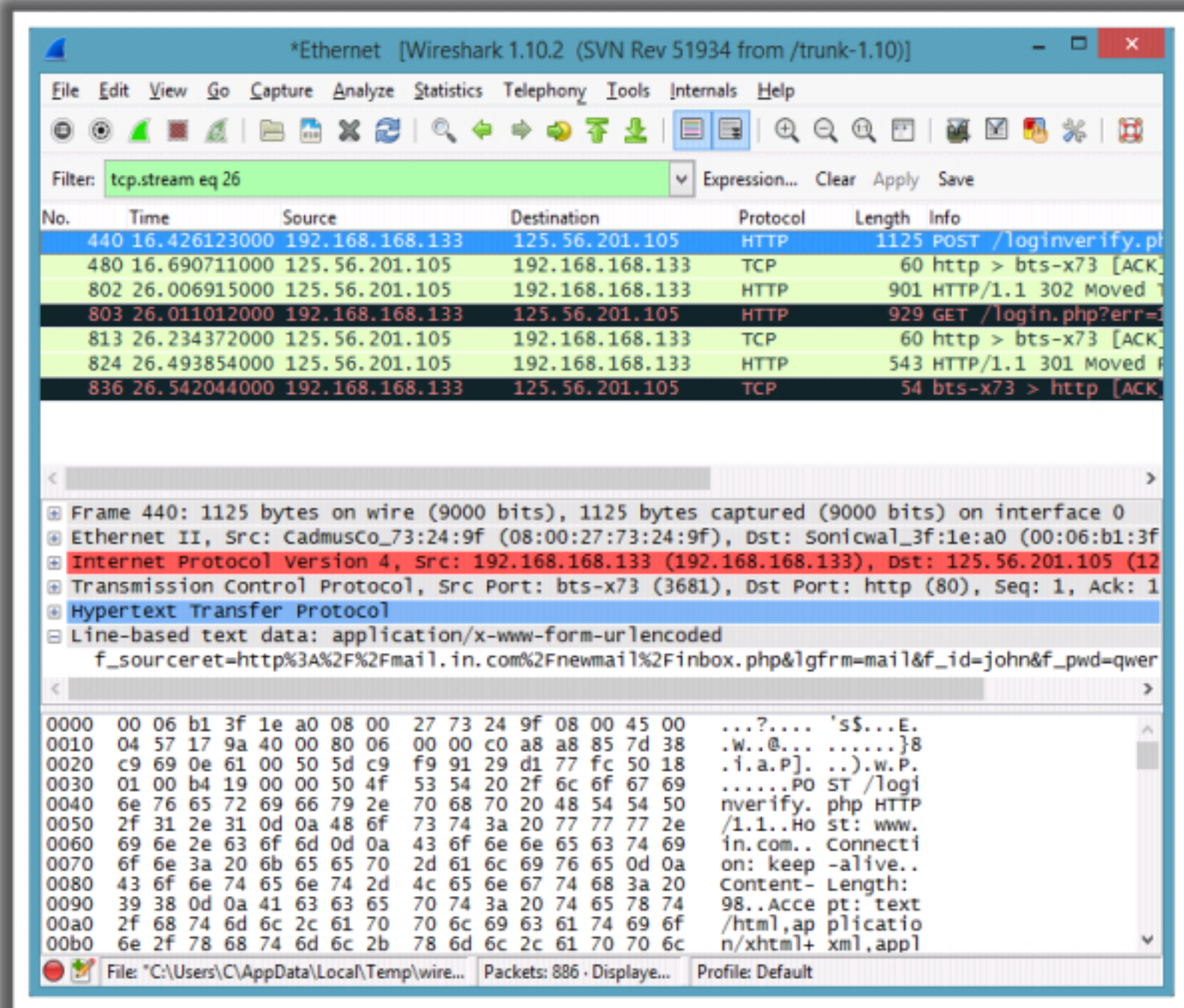


FIGURE 7.3: Screenshots showing the filtered packets

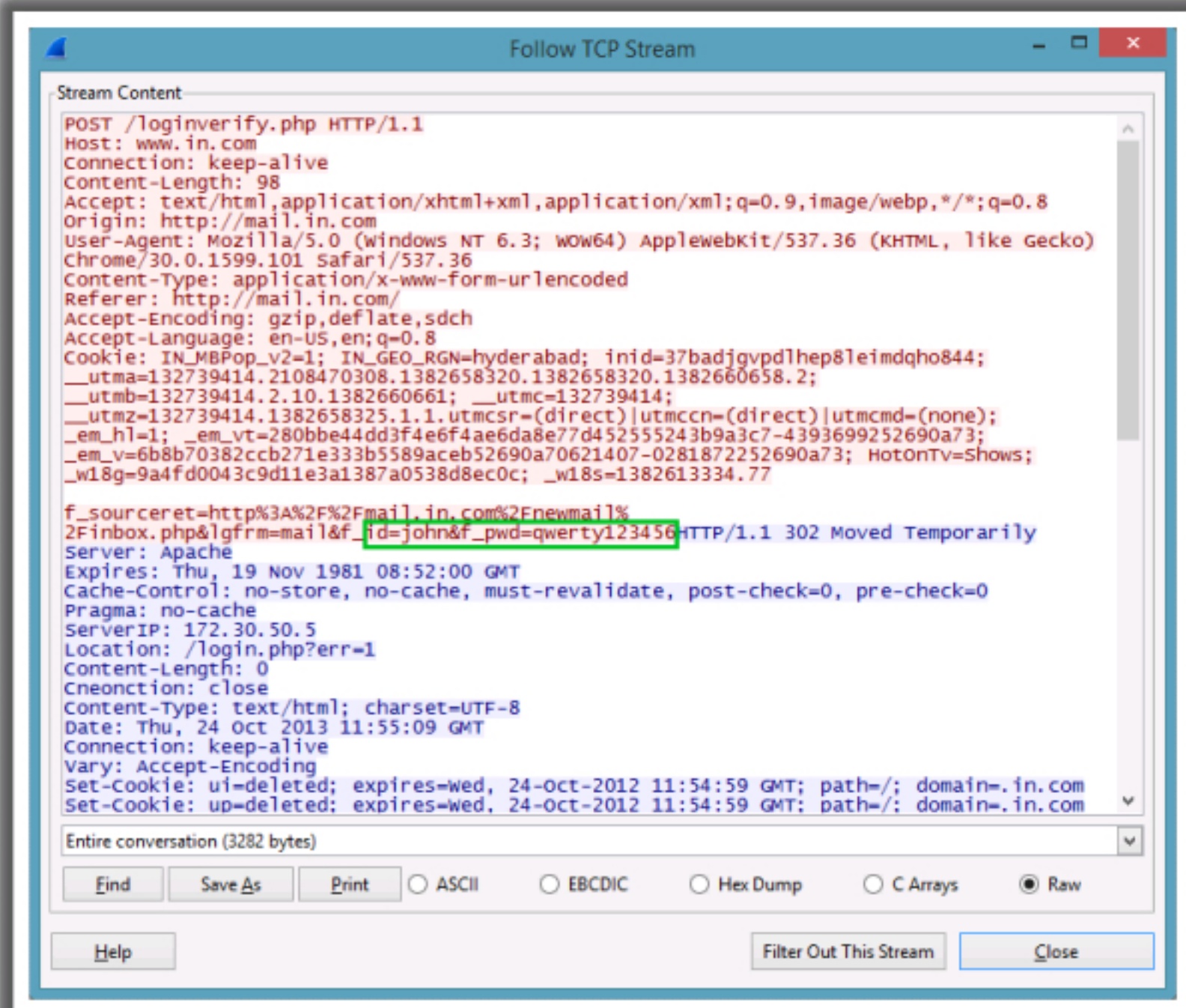








FIGURE 7.4: Screenshots showing the analysis of TCP stream



# Display Filters in Wireshark



Display filters are used to **change the view of packets** in the captured files

1	<b>Display Filtering by Protocol</b>	E.g.: Type the protocol in the filter box; arp, http, tcp, udp, dns, ip	
2	<b>Monitoring the Specific Ports</b>	<pre>tcp.port==23 ip.addr==192.168.1.100 machine ip.addr==192.168.1.100 &amp;&amp; tcp.port=23</pre>	
3	<b>Filtering by Multiple IP Addresses</b>	<pre>ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5</pre>	
4	<b>Filtering by IP Address</b>	<pre>ip.addr == 10.0.0.4</pre>	
5	<b>Other Filters</b>	<pre>ip.dst == 10.0.1.50 &amp;&amp; frame.pkt_len &gt; 400 ip.addr == 10.0.1.12 &amp;&amp; icmp &amp;&amp; frame.number &gt; 15 &amp;&amp; frame.number &lt; 30 ip.src==205.153.63.30 or ip.dst==205.153.63.30</pre>	

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Source: <http://wiki.wireshark.org>

Wireshark features a vast array of display filters. They allow drilldown to the exact traffic needed and are the basis of many Wireshark features.

### Display filtering by protocol:

Type the protocol in the Filter box, for example: `arp, http, tcp, udp, dns`

### Monitoring the specific ports:

```
tcp.port==23
```

```
ip.addr==192.168.1.100 machine ip.addr==192.168.1.100 &&tcp.port=23
```

### Filtering by multiple IP addresses:

```
ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5
```

### Filtering by IP address:

```
ip.addr == 10.0.0.4
```

### Other filters:

```
ip.dst == 10.0.1.50 &&frame.pkt_len > 400
```

```
ip.addr == 10.0.1.12 &&icmp&&frame.number > 15 &&frame.number < 30
```

```
ip.src==205.153.63.30 or ip.dst==205.153.63.30
```



# Additional Wireshark Filters




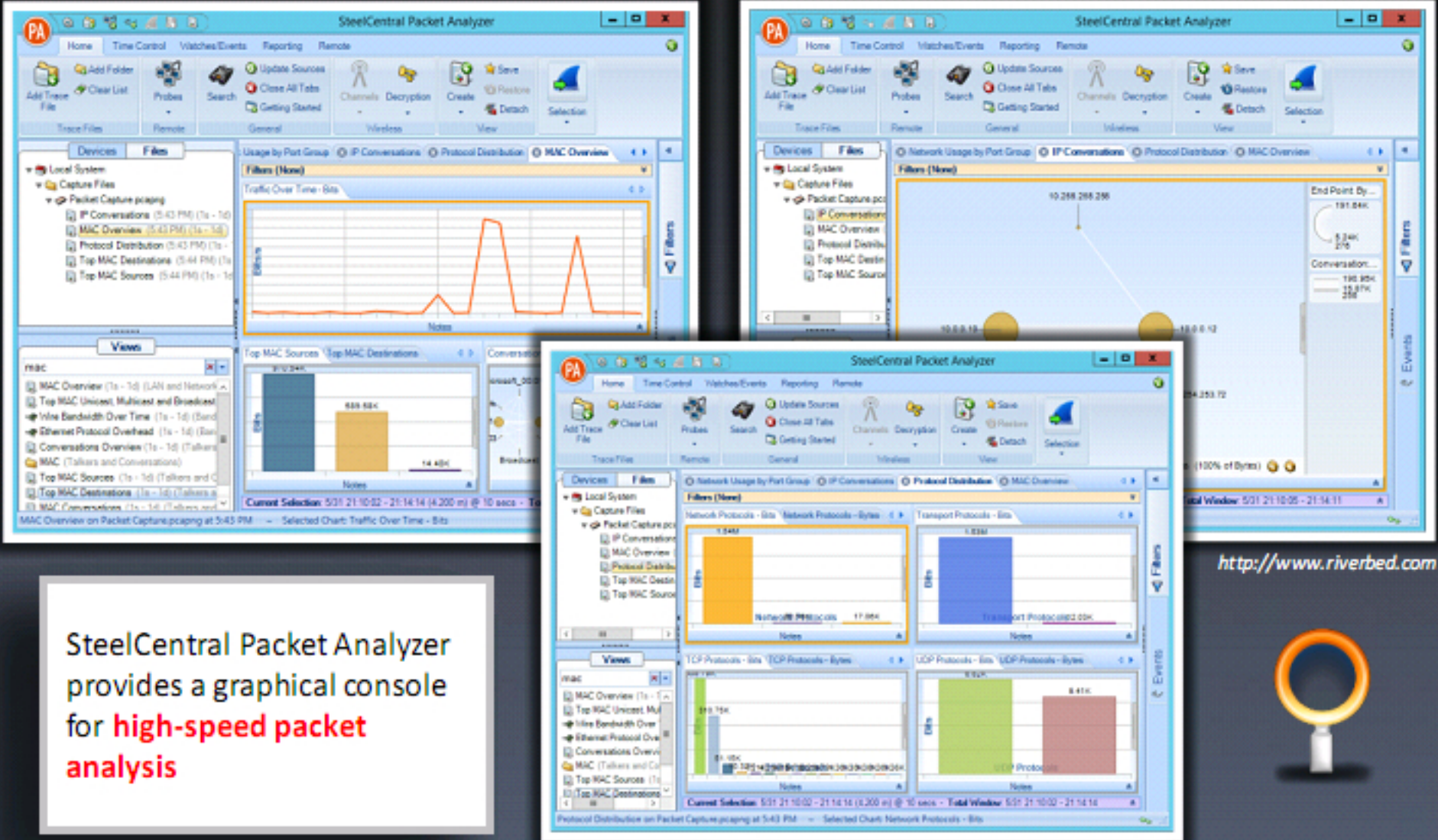
01	<code>tcp.flags.reset==1</code> Displays all TCP resets	
02	<code>udp contains 33:27:58</code> Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset	
03	<code>http.request</code> Displays all HTTP GET requests	
04	<code>tcp.analysis.retransmission</code> Displays all retransmissions in the trace	
05	<code>tcp contains traffic</code> Displays all TCP packets that contain the word 'traffic'	
06	<code>!(arp or icmp or dns)</code> Masks out arp, icmp, dns, or other protocols and allows you to view traffic of you interest	

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.



# Sniffing Tool: SteelCentral Packet Analyzer





SteelCentral Packet Analyzer provides a graphical console for **high-speed packet analysis**

<http://www.riverbed.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

SteelCentral Packet Analyzer is a packet analysis and reporting solution with an intuitive graphical user interface. We can use this tool with locally-presented trace files or remote SteelCentral™ NetShark devices, or SteelHead/SteelFusion running NetShark. SteelCentral Packet Analyzer identifies and troubleshoots network and application performance issues down to the bit level through Packet Analyzer's full integration with Wireshark.


### Features:

- High-speed packet analysis to rapidly detect problems
- Analyze multi-terabyte files quickly
- Professional reporting that everyone can understand
- No charge for multi-segment analysis
- Seamless integration with Wireshark

Source: <http://www.riverbed.com>



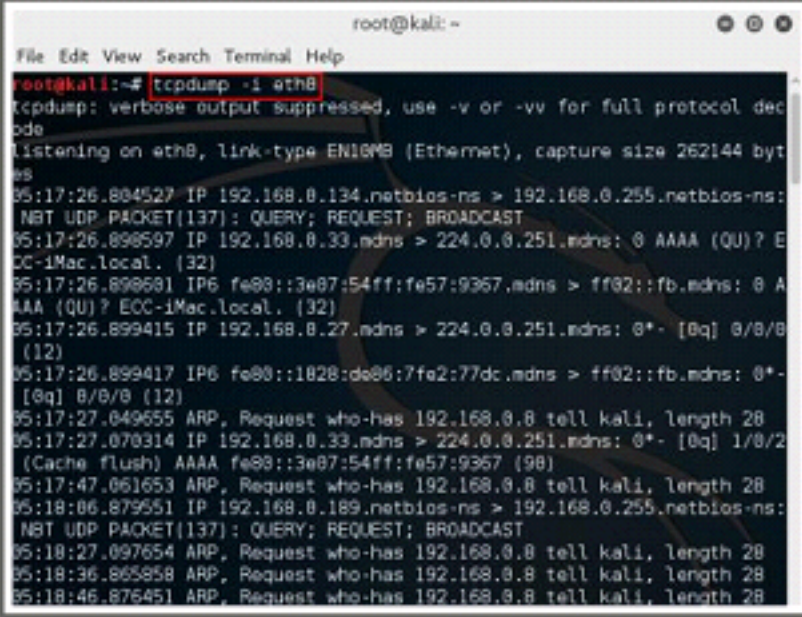
# Sniffing Tool: **Tcpdump/Windump**



TCPdump is a **command line interface packet sniffer** which runs on Linux and Windows

## TCPDump

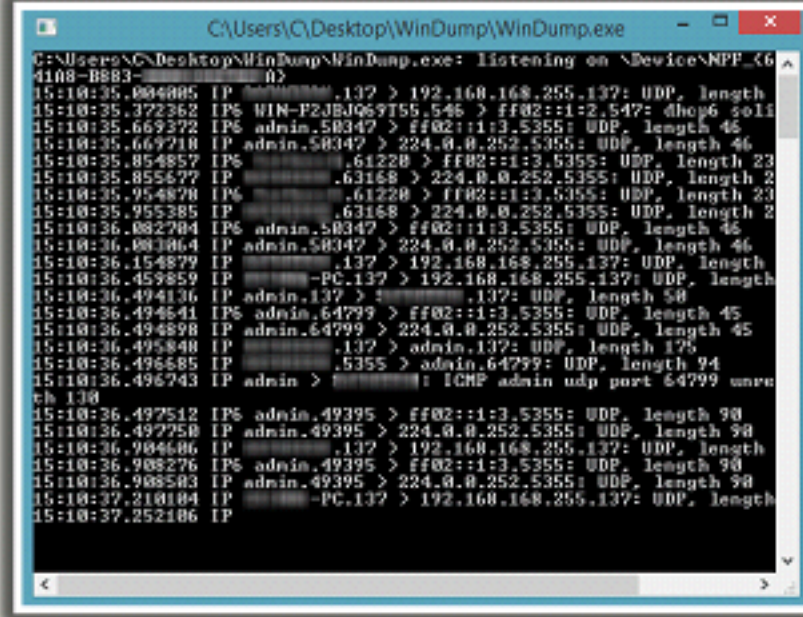
Runs on Linux and UNIX systems



<http://www.tcpdump.org>

## WinDump

Runs on Windows systems



<http://www.winpcap.org>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Tcpdump

Source: <http://www.tcpdump.org>

Tcpdump prints out a description of the contents of packets on a network interface that match the Boolean expression. It can run with the **-w** flag, which causes it to save the packet data to a file for later analysis, and/or with the **-r** flag, which causes it to read from a saved packet file rather than read packets from a network interface. In all cases, tcpdump processes only packets that match the expression.

Tcpdump will, if not run with the **-c** flag, continue capturing packets until it is interrupted by a SIGINT signal (generated, for example, by typing your interrupt character, typically control-C) or a SIGTERM signal (typically generated with the kill(1) command); if run with the **-c** flag, it will capture packets until it is interrupted by a SIGINT or SIGTERM signal or if the specified number of packets have been processed.

When tcpdump finishes capturing packets, it will report counts of:

- Packets “captured” – This is the number of packets that tcpdump has received and processed.
- Packets “received by filter” – The meaning of this depends on the OS running tcpdump, and possibly on the way the OS was configured. If a filter was specified on the command line:



- On some OSes, it counts packets regardless of whether the filter expression matches them or not and, even if they were matched by the filter expression, regardless of whether tcpdump has read and processed them yet.
- On some OSes, it counts only packets matched by the filter expression regardless of whether tcpdump has read and processed them yet.
- On some OSes, it counts only packets matched by the filter expression and processed by tcpdump).
- Packets “dropped by kernel” is the number of packets that were dropped due to a lack of buffer space, by the packet capture mechanism in the OS running tcpdump, if the OS reports that information to applications; if the information is not reported, it will be reported as 0.
- On platforms that support the SIGINFO signal, such as most BSDs (including Mac OS X) and Digital/Tru64 UNIX, it will report those counts when it receives a SIGINFO signal (generated, for example, by typing the “status” character, typically control-T, although on some platforms, such as Mac OS X, the “status” character is not set by default; then, the user must set it with sty (1) in order to use it) and will continue capturing packets.

```
tcpdump -i eth0
```

```
13:13:48.437836 10.20.21.03.router > RIP2-ROUTERS.MCAST.NET.router:  RIPv2
13:13:48.438364 10.20.21.23 > 10.20.21.55: icmp: RIP2-ROUTERS.MCAST.NET udp
13:13:54.947195 vmt1.endicott.juggyboy.com.router > RIP2-ROUTERS.MCAST.NET.rou
13:13:58.313192 :: > ff02::1:ff00:11: icmp6: neighbor sol: who has fe80::
13:13:59.313573 fe80::26f:5a00:100:11 > ipv6-allrouters: icmp6: router so
13:14:05.179268 :: > ff02::1:ff00:14: icmp6: neighbor sol: who has fe80::
13:14:06.179453 fe80::26f:5a00:100:14 > ipv6-allrouters: icmp6: router so
13:14:18.473315 10.20.21.55.router > RIP2-ROUTERS.MCAST.NET.router:  RIPv2
13:14:18.473950 10.20.21.23 > 10.20.21.55: icmp: RIP2-ROUTERS.MCAST.NET udp
13:14:20.628769 10.20.21.64.filenet-tms > btvdns01.srv.juggyboy.com.domain:  49
13:14:24.982405 vmt1.endicott.juggyboy.com.router > RIP2-ROUTERS.MCAST.NET.rou
```

## WinDump

Source: <http://www.winpcap.org>

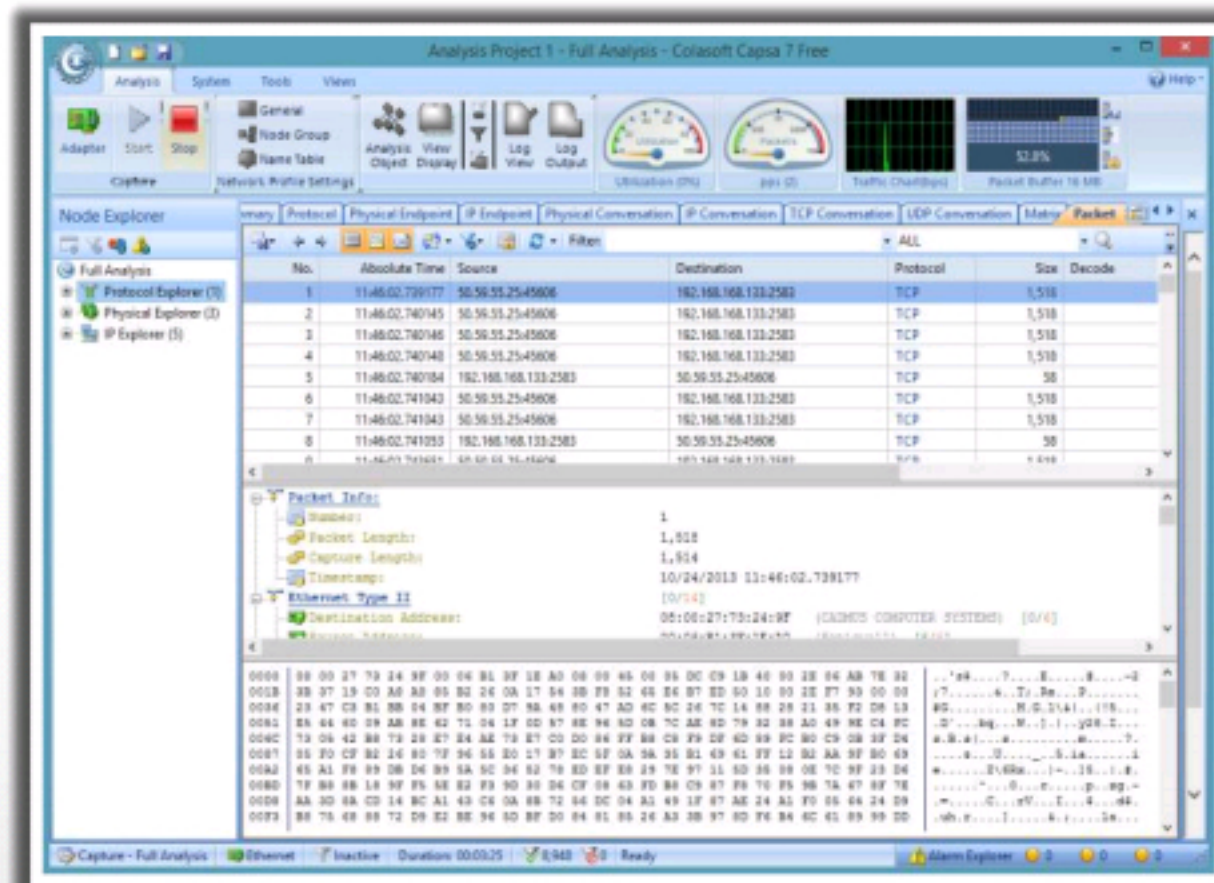
WinDump is the Windows version of tcpdump, the command line network analyzer for UNIX. WinDump is fully compatible with tcpdump and is used to watch, diagnose, and save to disk network traffic according to various complex rules. It can run under Windows 95, 98, ME, NT, 2000, XP, 2003, and Vista.



# Packet Sniffing Tool: Capsa Network Analyzer



Capsa Network Analyzer captures all data transmitted over the network and provides a wide range of analysis statistics in an intuitive and graphical way



<http://www.colasoft.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Capsa is a portable network analyzer for both LAN and WLAN that performs packet capturing, network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It provides visibility to the entire network, and helps network administrators or network engineers pinpoint and resolve various application problems.

## Features:

- Identify and analyze more than 300 network protocols, as well as network applications based on the protocols.
- Monitor network bandwidth and usage by capturing data packets transmitted over the network and providing summary and decoding information about these packets.
- View network statistics, allowing capture and interpretation of network utilization data.
- Monitor Internet, email, and instant messaging traffic, helping keep employee productivity to a maximum.
- Diagnose and pinpoint network problems by detecting and locating suspicious hosts.
- Map out the details, including traffic, IP address, and MAC of each host on the network, allowing for easy identification of each host and the traffic that passes through each.
- Visualize the entire network in an ellipse that shows the connections and traffic between each host.

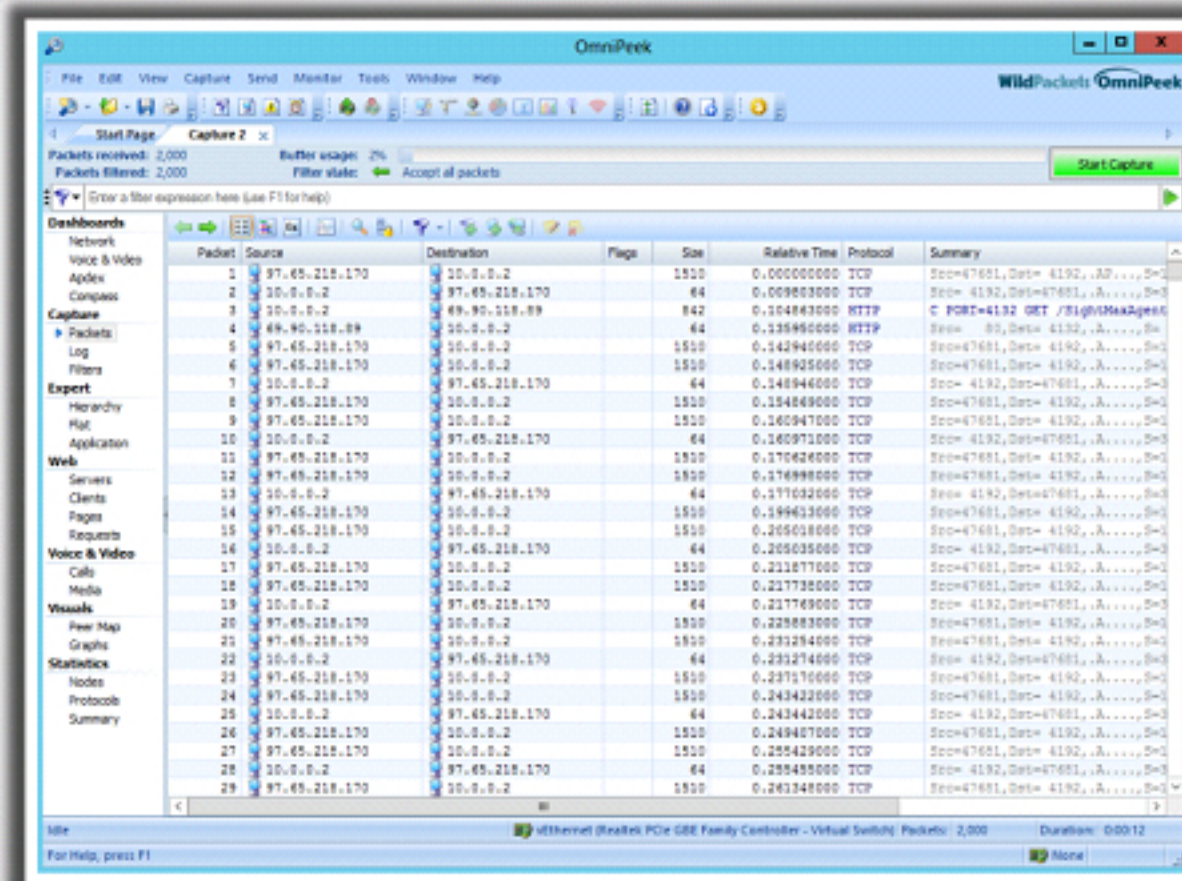
Source: <http://www.colasoft.com>



# Network Packet Analyzer: OmniPeek Network Analyzer



- OmniPeek sniffer displays a Google Map in the OmniPeek capture window showing the **locations of all the public IP addresses of captured packets**
- This feature is a great way to monitor the network in real time, and track that **traffic**



<http://www.wildpackets.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OmniPeek gives network engineers real-time visibility and expert analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and video to remote offices. By using OmniPeek's intuitive user interface and the "top-down" approach to visualize network conditions, network engineers can analyze, drill down and fix performance bottlenecks across multiple network segments, maximizing uptime and user satisfaction.

## Features:

- Network performance management and monitoring of networks, including network segments at remote offices
- Monitoring of key network statistics in real time, aggregating multiple files, and instantly drilling down to packets using the "Compass" interactive dashboard
- Seamless management of all OmniEngine software probes, and Omnipliance and TimeLine network recorders in the network
- Integrated support for Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless (including 3-stream), VoIP, video, MPLS, and VLAN
- Intuitive drill-down to understand which nodes are communicating, which protocols and sub-protocols are being transmitted, and which traffic characteristics are affecting network performance




- Complete voice and video over IP real-time monitoring, including high-level multimedia dashboard, call data record (CDR) and comprehensive signaling and media analyses

---

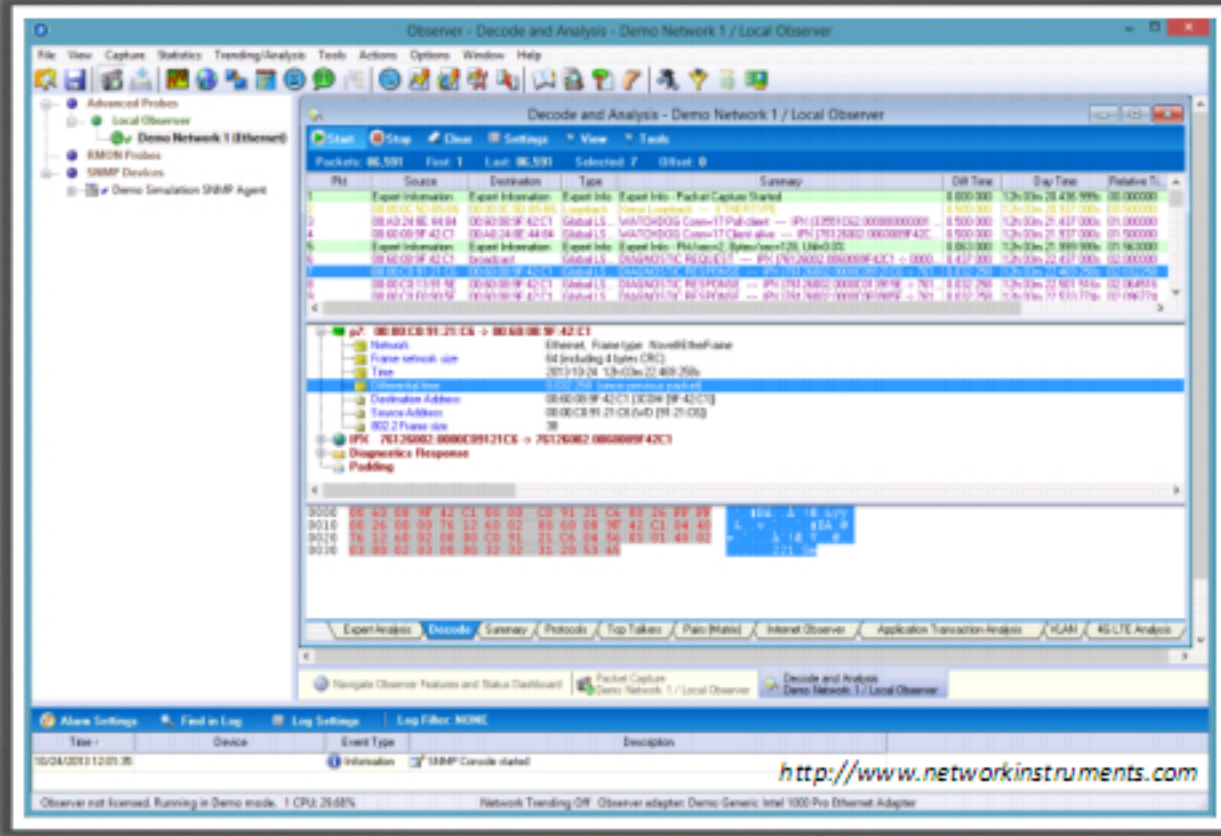
Source: <http://www.wildpackets.com>



# Network Packet Analyzer: Observer



Observer provides a comprehensive drill-down into network traffic and provides **back-in-time analysis**, reporting, trending, alarms, application tools, and **route monitoring capabilities**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Observer is a software used for troubleshooting in a network. It has features such as expert analysis, VoIP tools, in-depth application analysis, connection dynamics, stream reconstruction, and more, in addition to offering support for SNMP and RMON device management.

Users can generate and share reports via the web, add custom decode modules for use in proprietary environments, and extract data from external sources using SOAP.

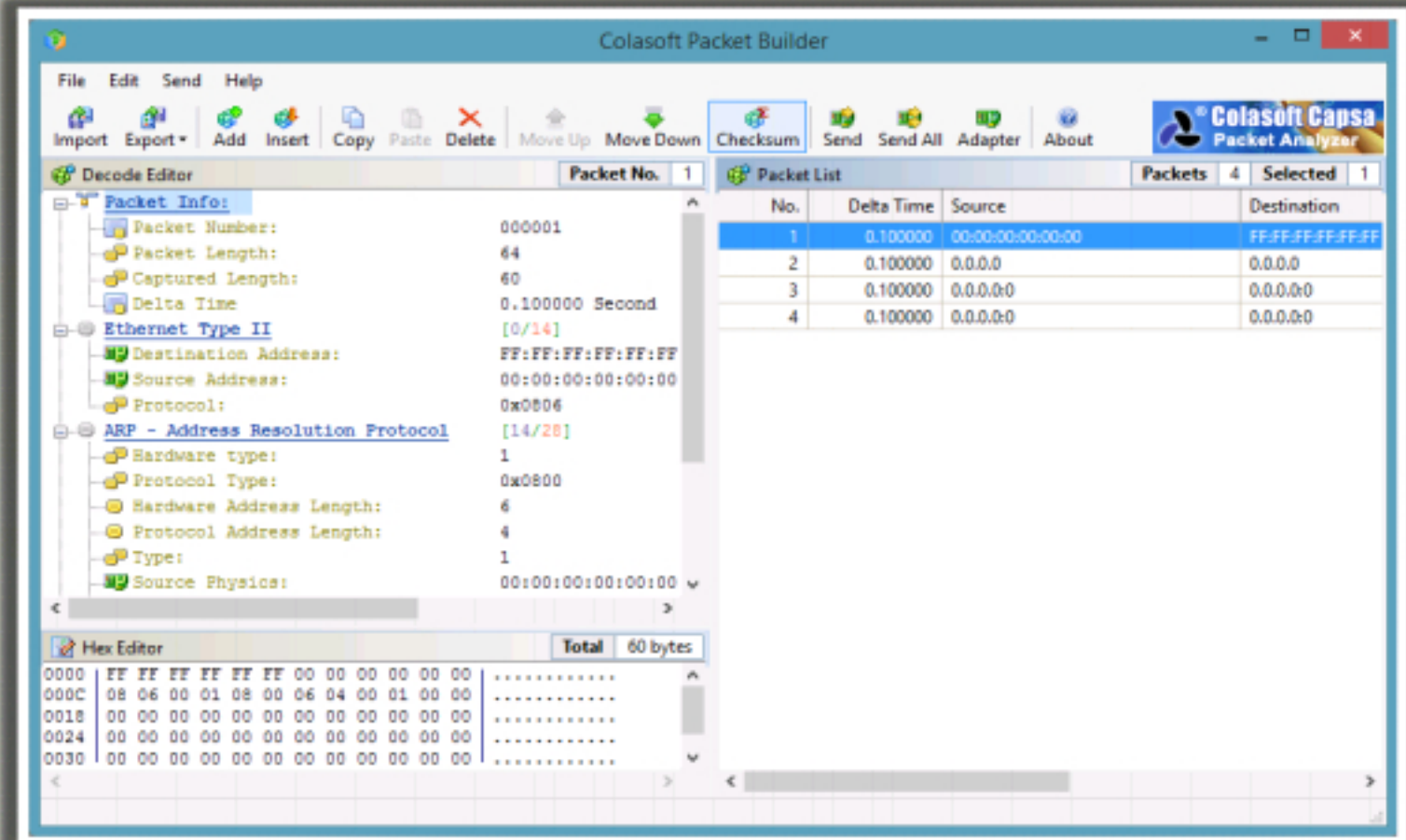
Source: <http://www.netinst.com>



# TCP/IP Packet Crafter: Colasoft Packet Builder



Colasoft Packet Builder allows user to select one from the provided templates: **Ethernet Packet**, **ARP Packet**, **IP Packet**, **TCP Packet** and **UDP Packet**, and **change the parameters** in the decoder editor, hexadecimal editor, or ASCII editor to create a packet



No.	Delta Time	Source	Destination
1	0.100000	00:00:00:00:00:00	FF:FF:FF:FF:FF:FF
2	0.100000	0.0.0.0	0.0.0.0
3	0.100000	0.0.0.0	0.0.0.0
4	0.100000	0.0.0.0	0.0.0.0

<http://www.colasoft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Colasoft Packet Builder enables creating custom network packets; users can use this tool to check the network protection against attacks and intruders. The tool includes an editing feature. Besides allowing common HEX editing of raw data, it features a decoding editor that allows for editing-specific protocol field values.

The users can edit decoding information in two editors: Decode Editor and Hex Editor. The tool allows users to select one of the provided templates Ethernet Packet, ARP Packet, IP Packet, TCP Packet, and UDP Packet, and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet.

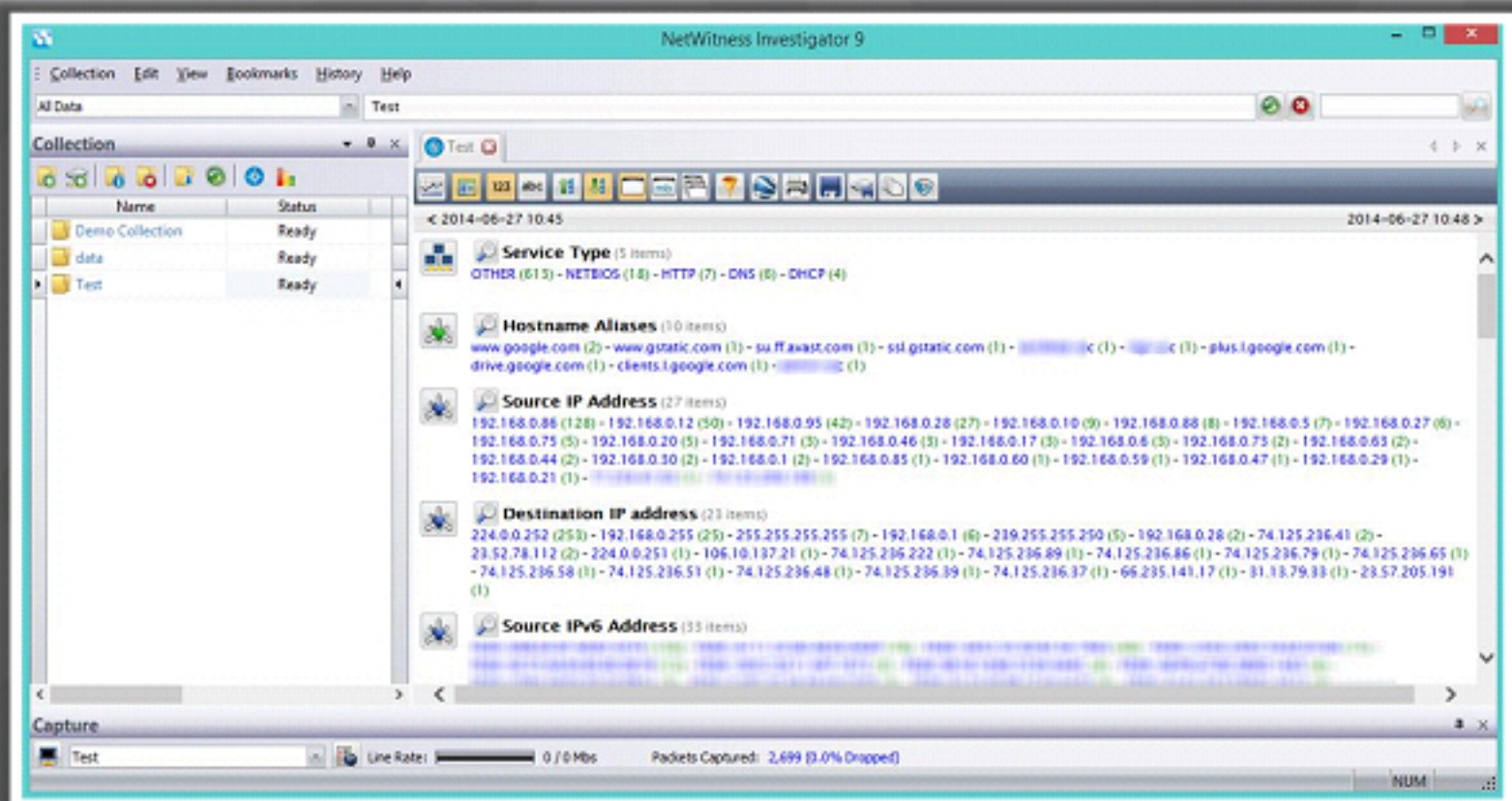
Source: <http://www.colasoft.com>



# Network Packet Analyzer: RSA NetWitness Investigator



**RSA NetWitness Investigator captures live traffic and process packet files from virtually any existing network collection devices**



<http://www.emc.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

NetWitness Investigator captures live traffic and processes packet files from virtually any existing network collection device for analysis. The tool can locally process packet files and record in real time from a network tap or span port with immediate insight into network traffic. The tool is the primary interactive application of the NetWitness AppSuite.

Source: <http://www.emc.com>



**Additional Sniffing Tools**



 <b>Ace Password Sniffer</b> <a href="http://www.ettech.com">http://www.ettech.com</a>	 <b>EffeTech HTTP Sniffer</b> <a href="http://www.ettech.com">http://www.ettech.com</a>
 <b>IPgrab</b> <a href="http://ipgrab.sourceforge.net">http://ipgrab.sourceforge.net</a>	 <b>ntopng</b> <a href="http://www.ntop.org">http://www.ntop.org</a>
 <b>Big Mother</b> <a href="http://www.tupsoft.com">http://www.tupsoft.com</a>	 <b>Ettercap</b> <a href="http://ettercap.sourceforge.net">http://ettercap.sourceforge.net</a>
 <b>EtherDetect Packet Sniffer</b> <a href="http://www.etherdetect.com">http://www.etherdetect.com</a>	 <b>SmartSniff</b> <a href="http://www.nirsoft.net">http://www.nirsoft.net</a>
 <b>dsniff</b> <a href="https://www.monkey.org">https://www.monkey.org</a>	 <b>EtherApe</b> <a href="http://etherape.sourceforge.net">http://etherape.sourceforge.net</a>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Ace Password Sniffer

Source: <http://www.ettech.com>

Ace Password Sniffer is a password recovery utility that captures the forgotten passwords. It is used to monitor the web activities and monitor password abuse. The tool supports and captures passwords through http, ftp, smtp, pop3, and telnet, including some web mail password. Ace Password Sniffer works passively and does not generate any network traffic; therefore, it is very hard for others to detect it. The tool requires any additional software on the target PCs or workstations if the network is connected through switch, thereby allowing the user to run the sniffer on the gateway or proxy server, which bears all network traffic.

It also acts as a stealth-monitoring utility and is useful to recover the network passwords, to receive network passwords of children for parents, and to monitor passwords abuse for server administrators.

## IPgrab

Source: <http://ipgrab.sourceforge.net>

IPgrab is a verbose packet sniffer for UNIX hosts.



## Big Mother

Source: <http://www.tupsoft.com>

Big Mother is a switchsniff with zero configurations used as an internet activity monitoring tool. Big Mother is an eavesdropping program that uses a switch sniffer to capture and analyze communication traffic over a network. The tool not only logs in real time URL visits, email, chats, games, FTP, and data flows but also takes webpage snapshots, duplicates email and FTP copies, records MSN messenger content, and gives statistical reports. It freely restricts online activities with time schedules and according to customized filtering Internet rules.

The program will set up itself and perform content monitoring and access control to keep family members or employees accountable for their actions.

## EtherDetect Packet Sniffer

Source: <http://www.etherdetect.com>

EtherDetect Packet Sniffer is a sniffing tool that can capture full packets organized by TCP connections or UDP threads and passively monitor the network, with any program installations on target PCs. The tool enables packet viewing in Hex format and syntax highlighting viewer.

Features:

- Organizes captured packets in a connection-oriented view
- Captures IP packets on the LAN with nearly no packets losing.
- Functions as a real-time analyzer, enabling on-the-fly content viewing while capturing and analyzing.
- Enables parse and decode a variety of network protocol.
- Supports saving captured packets for reopening afterward.
- Allows syntax highlighting for application data in the format of HTML, HTTP, and XML.

## dsniff

Source: <http://monkey.org>

dsniff is a tool for network auditing and penetration testing. Dsniff passively monitors a network for data, passwords, e-mail, files, etc. Further, arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker. Moreover, sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

## EffeTech HTTP Sniffer

Source: <http://www.efeotech.com>

EffeTech HTTP Sniffer is a HTTP packet sniffer, protocol analyzer, and file reassembly software based on windows platform. Unlike most other sniffers, this sniffer dedicates itself to capture IP packets containing HTTP protocol, rebuild the HTTP sessions, and reassemble files sent through HTTP protocol. Its smart real-time analyzer enables on-the-fly content viewing and captures, analyzes, parses, and decodes HTTP protocol.



By delivering an easy to use and award-winning HTTP monitoring utility, the EffeTech HTTP sniffer has become the preferred choice of managers, network administrators, and developers worldwide. Information about HTTP traffic can be received by all via LAN.

## Ntopng

Source: <http://www.ntop.org>

Ntopng is a network traffic probe that shows the network usage, similar to what the popular `top` Unix command does. Ntopng is based on `libpcap`, and it runs on every Unix platform, MacOSX and on Windows. Ntopng users utilize a web browser to navigate through ntop (that acts as a web server) traffic information and get a dump of the network status. In the latter case, ntopng acts as a simple RMON-like agent with an embedded web interface.

### Features:

- Sorts network traffic according to many criteria, including IP address, port, L7 protocol, throughput, AS.
- Shows network traffic and IPv4/v6 active hosts.
- Produces reports about various network metrics such as throughput, application protocols
- Stores on disk persistent traffic statistics in RRD format
- Geo-locates hosts and displays reports according to host location
- Characterizes HTTP traffic by leveraging on characterization services provided by Google and HTTP Blacklist.
- Shows IP traffic distribution among the various protocols
- Analyses IP traffic and sorts it according to the source/destination.
- Produces HTML5/AJAX network traffic statistics.

## Ettercap

Source: <http://ettercap.sourceforge.net>

Ettercap is a comprehensive suite for man-in-the-middle attacks. The tool features sniffing of live connections, content filtering on the fly, and many other interesting tricks. Ettercap supports active and passive dissection of many protocols and includes many features for network and host analysis.

## SmartSniff

Source: <http://www.nirsoft.net>

SmartSniff is a network monitoring utility that captures TCP/IP packets that pass through the network adapter and displays the captured data as a sequence of conversations between clients and servers. The tool allows viewing the TCP/IP conversations in Ascii or as hex dump.




## EtherApe











Source: <http://etherape.sourceforge.net>

EtherApe is a graphical network monitor for UNIX modeled after etherman. The tool features link layer, IP and TCP modes, and graphically displays network activity. Hosts and links change in size with traffic. Color-coded protocols display. EtherAPE supports Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP and WLAN devices, plus several encapsulation formats. It can filter traffic and can read packets from a file as well as live from the network. It can also export node statistics.



**Additional Sniffing Tools (Cont'd)**



 <b>Network Probe</b> <a href="http://www.objectplanet.com">http://www.objectplanet.com</a>	 <b>CommView</b> <a href="http://www.tamos.com">http://www.tamos.com</a>
 <b>WebSiteSniffer</b> <a href="http://www.nirsoft.net">http://www.nirsoft.net</a>	 <b>NetResident</b> <a href="http://www.tamos.com">http://www.tamos.com</a>
 <b>ICQ Sniffer</b> <a href="http://www.etherboss.com">http://www.etherboss.com</a>	 <b>Kismet</b> <a href="http://www.kismetwireless.net">http://www.kismetwireless.net</a>
 <b>MaaTec Network Analyzer</b> <a href="http://www.maatec.com">http://www.maatec.com</a>	 <b>AIM Sniffer</b> <a href="http://www.ettech.com">http://www.ettech.com</a>
 <b>Alchemy Eye</b> <a href="http://www.alchemy-lab.com">http://www.alchemy-lab.com</a>	 <b>NetworkMiner</b> <a href="http://www.netresec.com">http://www.netresec.com</a>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

## Network Probe

Source: <http://www.objectplanet.com>

Network Probe is the network monitor and protocol analyzer to monitor network traffic tool. It can find the sources of any network slow-downs. The tool displays the protocols used on your network, which hosts are sending and receiving data, where the traffic is coming from, and when all this happens. The Network Probe allows configuring in such a way that it can notify if anything out of the ordinary happens and can proactively fix the problem before it grows into a serious one

## WebSiteSniffer

Source: <http://www.nirsoft.net>

WebSiteSniffer is a packet sniffer tool to capture all Web site files downloaded by the Web browser while browsing the Internet and stores them on your hard drive under the base folder that you choose. WebSiteSniffer allows the users to capture any required type of Web site files: HTML Files, Text Files, XML Files, CSS Files, Video/Audio Files, Images, Scripts, and Flash (.swf) files. While capturing the Web site files, the main window of WebSiteSniffer displays general statistics about the downloaded files for every Web site/host name, including the total size of all files (compressed and uncompressed) and total number of files for every file type.



## ICQ Sniffer

Source: <http://www.etherboss.com>

ICQ Sniffer is a network utility that can capture and log ICQ chat from computers within the same LAN. It supports messaging through ICQ server with format of plain text, RTF, or HTML. It provides a report system to export captured ICQ conversations as HTML files for later analysis and reference.

## MaaTec Network Analyzer

Source: <http://www.maatec.com>

The MaaTec Network Analyzer is a tool that allows capturing, saving, and analyzing network traffic on a LAN or a DSL internet connection. We can use this tool for network troubleshooting, to analyze the existing network infrastructure, or for long-term network monitoring.

### Features:

- Unique new packet information display in split window
- Supports multiple network cards in one or multiple windows
- Reports with charts and multiple data tables
- Provides support for files that are larger than 2 GB
- Enables online view of incoming packets

## Alchemy Network Monitor

Source: <http://www.mishelpers.com>

Alchemy Eye monitors network server availability and performance. It supports over 50 monitoring types, including, but not limited to ICMP ping, NT Event Log monitoring, HTTPS/FTP URL checking, free disk space monitoring, etc. Alchemy Eye notifies the Network Administrator about server malfunction events. It logs application events to a log file. Different log file detail levels (none/normal/full) and log file formats (text, HTML, CSV, SQL database) can be configured using the application.

## CommView

Source: <http://www.alchemy-lab.com>

CommView is a network monitor and analyzer designed for LAN administrators, security professionals, network programmers, home users, and anyone who wants a full picture of the traffic flowing through a PC or LAN segment. The application captures every packet on the wire to display important information such as a list of packets and network connections, vital statistics, and protocol distribution charts.

CommView allows the users to examine, save, filter, import, and export captured packets, view protocol decodes down to the lowest layer with full analysis of supported protocols. With the information, CommView can help the users pinpoint network problems and troubleshoot software and hardware.



## NetResident

Source: <http://www.tamos.com>

NetResident is a network content analysis application designed to monitor, store, and reconstruct network events and activities, such as e-mail messages, web pages, downloaded files, instant messages, and VoIP conversations. NetResident saves the data to a database, reconstructs it, and displays the content in a simple format.

### Features

- In-depth, real-time view of network traffic and storage of data in a database
- Deep packet inspection: state-of-the-art technology for searching, identifying, and reconstructing many protocols and data types: HTTP, POP3, SMTP, FTP, News, VoIP (SIP, H.323), IM (MSN, Yahoo, ICQ, etc.), Web Mail (Gmail, Hotmail, etc.), Telnet
- Customizable alerts: pop-ups, e-mail notifications, SNMP traps, to name a few
- Log file import in popular formats for post-capture forensic analysis: PCAP, CommView, etc.

## Kismet

Source: <http://www.kismetwireless.net>

Kismet is a wireless network detector, sniffer, and intrusion detection system. Kismet works predominately with Wi-Fi networks; however, we can expand it via plug-ins to handle other network types.

### Features include:

- Standard PCAP logging and multiple capture source support
- Plug-in architecture to expand core features
- Live export of packets to other tools via tun/tap virtual interfaces
- XML output for integration with other tools

## AIM Sniffer

Source: <http://www.efeotech.com>

AIM Sniffer is a network utility to capture and log AIM (AOL Instant Messenger) chat from computers within the same LAN. The tool supports messaging through AIM server and direct connection messaging. All intercepted messages are well organized by AIM user with buddies and shown instantly on the main window. It provides a features report system to export captured AIM conversations as HTML files for later analyzing and reference.


## NetworkMiner

Source: <http://www.netresec.com>

NetworkMiner is a Network Forensic Analysis Tool for Windows/Linux/Mac OS X/FreeBSD used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports, etc., without placing any traffic strain on the network. NetworkMiner can also parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files.



## Gathering Evidence from an IDS



An administrator can configure an IDS to **capture network traffic when an alert is generated**

However, this **data is not a sufficient source of evidence** because integrity checks cannot be performed on the log files

In a network investigation, preserving digital evidence is difficult, as data is **displayed on-screen for a few seconds**

Investigators can **record examination results** from networking devices such as routers, switches, and firewalls through a serial cable and software such as the Windows HyperTerminal program or a script on UNIX

If the amount of information to be captured is large, an investigator can **record the on-screen event** using a video camera or a related software program

The **disadvantage** of this method is that there is **no integrity check**, making it difficult to authenticate the information

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Monitoring network traffic is of prime importance. Organizations install IDSes to monitor intrusions. To capture network traffic, first configure the IDS. However, this is not sufficient as a source of evidence, because the IDS is incapable of performing integrity checks on log files. In a network investigation, preserving digital evidence is difficult, as the data displayed on screen will remain only for few seconds.

The Windows HyperTerminal program or Script can be used on UNIX through a serial cable to record the results of the examination of a networking device such as a router or switch.

If the amount of information required is large, we can record the onscreen event using a video camera or a relevant software program. This technique is useful for collecting dynamic digital evidence. We can later produce this evidence as a videotape. The disadvantage in such a program is that it does not perform an integrity check, making it difficult to authenticate the information.



## Documenting the Evidence Gathered on a Network



- ➔ Documenting the evidence gathered on a network is easy if the **network logs** are small, as a **printout** can be taken and attested
- ➔ Documenting **digital evidence** on a network becomes more complex when the evidence is gathered from systems located **remotely**, because of the unavailability of **date** and **time stamps** of the related files
- ➔ If the evidence resides on a **remote computer**, detailed information about collection and location should be **documented**. The investigator should specify the **server** containing the data to avoid confusion
- ➔ For documentation and integrity of the document, it is advisable to follow a **standard methodology**
- ➔ To support the **chain of custody**, the investigator should print out **screenshots** of important items and attach a record of actions taken during the **collection process**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Documenting the evidence gathered on a network is easy if the network logs are small, since it is possible to take and attest a printout. When we gather evidence from systems that are in remote locations, documenting the digital evidence on a network becomes more complex because of the unavailability of date and time stamps of the related files. If the evidence resides on a remote computer, it is important to document the detailed information about collection and location. The investigator should specify the server containing the data to avoid confusion. For proper documentation and maintaining the integrity of the document, it is advisable to follow a standard methodology. To support the chain of custody, the investigator should print out screenshots of important items and attach a record of the actions taken during the collection process.



# Evidence Reconstruction for Investigation



## Gathering evidence on a network is cumbersome for the following reasons:

- Evidence is not static and not concentrated at a single point on the network. The **variety of hardware and software** found on the network **makes the evidence-gathering process more difficult**
- Once the evidence is gathered, it can be used to **reconstruct the crime** to produce a clearer picture of the crime and identify the missing links in the picture

## Fundamentals of reconstruction for investigating a crime:

### Temporal analysis

It produces a sequential event trail, which sheds light on important factors such as what happened and who was involved

### Relational analysis

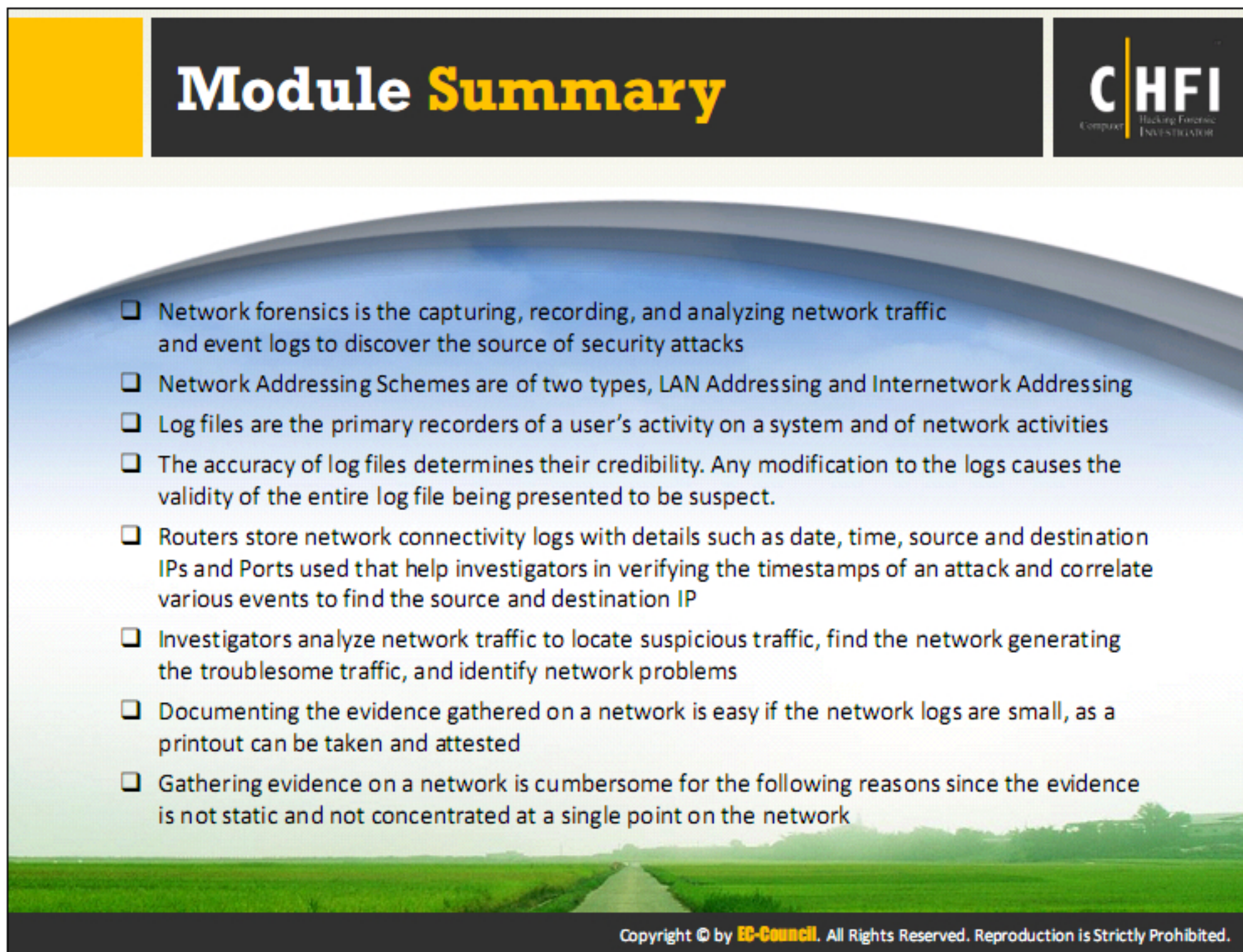
It correlates the actions of suspect and victim

### Functional analysis


It provides a description of the possible conditions of a crime. It testifies to the events responsible for a crime in relation to their functionalities

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.





# Module Summary



- ☐ Network forensics is the capturing, recording, and analyzing network traffic and event logs to discover the source of security attacks
- ☐ Network Addressing Schemes are of two types, LAN Addressing and Internetwork Addressing
- ☐ Log files are the primary recorders of a user's activity on a system and of network activities
- ☐ The accuracy of log files determines their credibility. Any modification to the logs causes the validity of the entire log file being presented to be suspect.
- ☐ Routers store network connectivity logs with details such as date, time, source and destination IPs and Ports used that help investigators in verifying the timestamps of an attack and correlate various events to find the source and destination IP
- ☐ Investigators analyze network traffic to locate suspicious traffic, find the network generating the troublesome traffic, and identify network problems
- ☐ Documenting the evidence gathered on a network is easy if the network logs are small, as a printout can be taken and attested
- ☐ Gathering evidence on a network is cumbersome for the following reasons since the evidence is not static and not concentrated at a single point on the network

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

In this module, we have discussed the importance of network forensics, and its role in performing a forensic investigation. This module introduced you to various topics related to network forensics, which will help you to examining various kinds of logs, gathering evidence, and reconstructing the evidence. This will help you in recreating the scene and tracking the accused, who is responsible for the incident.

In the next module, we will discuss the different web server architectures, various types of attacks occurring on web applications, and guidelines to investigate web attacks.